Univerzita Hradec Králové

Přírodovědecká fakulta

Filozofická fakulta

Možnosti zařazení tématu kryptoaktiva do RVP G

Bakalářská práce

Autor:	Marko Čermák
Studijní program:	B1801 – Informatika
Studijní obor:	Informatika se zaměřením na vzdělávání
	Společenské vědy se zaměřením na vzdělávání
Forma studia:	prezenční
Vedoucí práce:	Ing. Ivan Soukal, Ph.D.

Hradec Králové 2020

Univerzita Hradec Králové
Přírodovědecká fakulta

Zadání bakalářské práce

Autor:	**Marko Čermák**
Studium:	S19IN003BP
Studijní program:	B1801 Informatika
Studijní obor:	Informatika se zaměřením na vzdělávání, Společenské vědy se zaměřením na vzdělávání
Název bakalářské práce:	**Možnosti zařazení tématu kryptoaktiva do RVP G**
Název bakalářské práce AJ:	Cryptoassets topic at the grammar school

Cíl, metody, literatura, předpoklady:

Práce je zaměřena na možnosti zařezení tématu kryptoaktiv do RVP G vzdělávaící oblasti OSZ a IKT. Teoretická část vymezuje kryptoaktivum, rozdílnou podstatu fungování jednotlivých kryptoaktiv, tematické celky spojené s finanční gramotností a informačními technologiemi, didaktický základ k přípravě hodiny. Praktická část představuje modelové hodiny sloužící k vysvětlení vybraných aspektů kryptoaktiv.

Jaromír Veber. Digitalizace ekonomiky a společnosti : výhody, rizika, příležitosti. Praha : 2018

Boris Kaliský. Bitcoin a ti druzí : nepostradatelný průvodce světem kryptoměn. Praha : 2018

Andreas Cervenka. Peníze : jakou mají cenu? : --a čemu věřit v současném světě? Praha : 2014

Dominik Stroukal; Jan Skalický. Bitcoin a jiné kryptopeníze budoucnosti : historie, ekonomie a technologie kryptoměn, stručná příručka pro úplné začátečníky. Praha : 2018

Ivan Bertl. Finanční gramotnost : otázky a odpovědi, problémy a jejich řešení. Ústí nad Labem : 2018

Garantující pracoviště:	Katedra filosofie a společenských věd, Filozofická fakulta
Vedoucí práce:	Ing. Ivan Soukal, Ph.D.
Oponent:	doc. Mgr. Martin Paleček, Ph.D.

Datum zadání závěrečné práce: 13.2.2020

Prohlášení

Prohlašuji, že jsem bakalářskou práci zpracoval samostatně s použitím uvedené literatury.

V Hradci Králové dne: .....

Marko Čermák

Poděkování

Děkuji vedoucímu práce, panu Ing. Ivanu Soukalovi, Ph.D., za odborné vedení, vstřícnost projevenou při zpracování této bakalářské práce a jeho cenné rady a připomínky.

Anotace

ČERMÁK, Marko. *Možnosti zařazení tématu kryptoaktiva do RVP G*. Hradec Králové: Filozofická fakulta, Univerzita Hradec Králové, 2020. 92 s. Bakalářská práce.

Úvodní, teoretická, část této bakalářské práce se zaměřuje na vymezení pojmů české RVP G a objasnění definic týkajících se kryptoaktiv. V oblasti RVP G se práce zabývá aktuální podobou vyučování občanských a společenskovědních základů, člověk a svět práce, informačních a komunikačních technologií na gymnáziích. Téma kryptoaktiva je závislé na pochopení fungování peněz, centrálního systému bank, algoritmů, výpočetního výkonu a hardwaru. Cílem teoretické části je také definovat pojmy, které se používají ve světě kryptoaktiv. Stěžejní v této bakalářské práci je její praktická část, která se skládá z modelových hodin, ve kterých jsou probírána vybraná témata týkající se kryptoaktiv. Během hodin základů společenských věd získají žáci různých ročníků všeobecný přehled o principech a vlastnostech kryptoaktiv. V průběhu hodin informatiky získá žák technické znalosti o softwarových i hardwarových požadavcích k těžbě kryptoaktiv.

Klíčová slova: kryptoaktiva, rámcově vzdělávací program pro gymnázia, blockchain, modelové vyučovací hodiny

Annotation

ČERMÁK, Marko. *Cryptoassets topic at the grammar school*. Hradec Králové: Faculty of Arts, University of Hradec Králové, 2020. 92 pages. Bachelor Thesis.

The introductory, theoretical section of this bachelor's thesis focuses on defining the terms relating to the Czech framework educational program for grammar schools, and clarification of definitions related to crypto-active activities. In the field surrounding general educational programmes for grammar schools, the work includes teaching civic and social sciences, man and the world of work, alongside information and communication technology in grammar schools. Crypto-active activities depend on understanding the functioning of money, central systems of banks, algorithms, computing power and hardware. The theoretical part of this study will further aim to define the terms used in the world of crypto activities. Central to this bachelor's thesis is its didactic section, which consists of model lessons in which appropriately selected topics related to crypto-active activities are discussed. During the basic science classes, students of different grades will gain a general overview of the principles and properties of cryptoactive. During the computer science lessons, the student will gain technical knowledge of software and hardware requirements for the extraction of crypto-active.

Keywords: cryptoactive, framework educational program for grammar schools, blockchain, model lessons

Obsah

Úvod

Nové technologie a technologické postupy se staly pro náš každodenní život zcela nepostradatelnými. Již první lidé se snažili svůj běžný život zpříjemnit a ulehčit pomocí různých vynálezů. Myslím si, že touha po snadném životě v nás přežívá již po tisíciletí. Moderní civilizace jsou na technologiích závislé, proto je nezbytné novým technologiím rozumět a umět s nimi správně pracovat.

Jednou z nejrevolučnějších myšlenek posledního desetiletí jsou kryptoaktiva, jejichž aktuální podobu přirovnává článek (jrcornel 2018) k internetu v 80. letech. Používání internetu bylo označováno za náročné a komplikované, nicméně v dnešním světě si život bez něj nedokážeme představit. Užívání internetu otevřelo pomyslné dveře do globalizovaného světa a zásadně se přičinilo o stav dnešní společnosti.

V současné chvíli, kdy svět zasáhla pandemie COVID-19, se všichni obávají celosvětové krize. Tato pandemie nezmění jen způsob přemýšlení o zdraví, ale také o penězích (Leonard 2020).

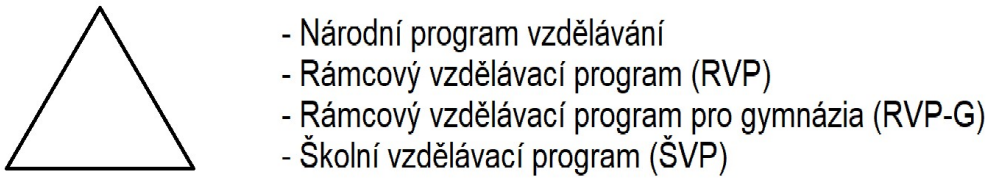
Znalost kryptoaktiv, které v dnešní době používá stále více lidí, by si měl osvojit minimálně každý student gymnázia (Tassev, 2019).

Teoretická část si klade za cíl zhodnotit aktuální podobu RVP G a shrnout klíčové znalosti k tématu kryptoaktiva. Mezi tyto znalosti patří znalost fungování a používání peněz a měn, znalost základních termínů typických pro kryptoaktiva, využití kryptoaktiv a decentralizovaných aplikací, princip těžby a fungování hashovací funkce. Teoretická část obsahuje příklady a vlastnosti konkrétních kryptoaktiv.

Praktická část obsahuje návrhy modelových hodin, které obsahují krátký úvod, bodově shrnuté cíle hodiny, rozvíjené klíčové kompetence, časovou dotaci, použité pomůcky, způsob hodnocení, způsob uchování informací, kontext vyučované lekce, časový harmonogram a detailní popis aktivit. Modelové hodiny budou odučeny na gymnáziích v Královéhradeckém a Pardubickém kraji. Během vyučování modelové hodiny bude přítomný pedagog, který daný předmět běžně vyučuje, ale nebude do hodiny zasahovat.

1 Vymezení Rámcového vzdělávacího programu pro gymnázia

Na základě školského zákona byl vytvořen systém kurikulárních dokumentů pro vzdělávání žáků od 3 do 19 let. Kurikulární dokumenty jsou státní a školní. Do státních kurikulárních dokumentů patří národní program vzdělávání (NVP) a rámcové vzdělávací programy (RVP). Národní vzdělávací program si klade za cíl formulovat požadavky na vzdělávání, které platí pro všechny školy, zatímco rámcově vzdělávací program vymezuje rámcové vzdělávací postupy pro jednotlivé etapy vzdělávání (Balada; et.al., 2007).



Obr. 1: Systém kurikulárních dokumentů – vlastní tvorba

1.1 Charakteristika RVP G

Jedná se o RVP, který se vztahuje pouze na vzdělávání na čtyřletých gymnáziích a na vyšším stupni víceletých gymnázií (Balada; et.al., 2007).

Poslední úprava RVP G proběhla v roce 2016. Toto opatření mění RVP G v bodech týkajících se vzdělávání žáků se speciálními vzdělávacími potřebami a vzdělávání nadaných a mimořádně nadaných žáků (Ministerstvo školství, 2016).

V oblasti systému péče o nadané a mimořárně nadané žáky je v nové úpravě RVP G věnována pozornost povinnosti školy vytvořit takové prostředí, které by vedlo k nejvyššímu využití potenciálu každého žáka s ohledem na jeho individuální možnosti, na jejichž základě je vypracován IVP. (Ministerstvo školství, 2016)

1.2 Kompetence v RVP G

Klíčové kompetence, na které RVP G klade důraz, jsou: kompetence k učení, kompetence k řešení problémů, kompetence komunikativní, kompetence sociální a personální, kompetence občanské, kompetence k podnikavosti. Tyto kompetence jsou souborem vědomostí a postojů, jež jsou důležité pro rozvoj jedince a jeho následné zapojení do společnosti. Kompetence v RVP G vycházejí z všeobecných kompetencí, které se

očekávají od absolventů gymnázií. Z důvodu jedinečnosti všech žáků je důležité, aby učitel plánoval osvojování kompetencí pro každého žáka individuálně (Balada; et.al., 2007).

Cílem kompetence k učení je rozvoj žákovy samostatnosti a plánovaní činnosti. Klade se důraz na jeho seberealizaci a osobní rozvoj. Po osvojení této kompetence by měl být žák schopen úspěšně aplikovat různé učící strategie a kritické myšlení ke zpracování informací. (Balada; et.al., 2007).

Kompetence k řešení problémů rozvíjí analytické a kritické myšlení. Žák by měl umět rozpoznat problém a navrhnout kroky k jeho vyřešení. Na základě již získaných znalostí a dovedností by měl být žák schopný kriticky zhodnotit svůj postup při řešení problému. (Balada; et.al., 2007).

Komunikativní kompetence zahrnuje verbální i neverbální komunikaci. Do komunikace patří symboly i grafy. Žák si po osvojení této kompetence dokáže srozumitelným a vhodným způsobem vyjádřit své myšlenky (Balada; et.al., 2007).

Při rozvoji sociální a personální kompetence žák dokáže aplikovat sebereflexi a posoudit své fyzické a duševní možnosti. Žák na základě svých schopností, dovedností, znalostí a zkušeností zaujímá postoje k sobě samému a ke společnosti. Žák si uvědomuje sílu vlastního jednání a přizpůsobuje ho různým situacím. Dále nepodléhá mediálnímu ani společenskému tlaku a rozhoduje se na základě vlastních priorit. Žák je veden k zodpovědnosti, toleranci a empatii (Balada; et.al., 2007).

Záměrem rozvoje občanské kompetence je prohloubit vztahy mezi osobními a veřejnými prioritami. Žák by měl být schopen podílet se na chodu společnosti, dbát na stav životního prostředí a kulturních památek. (Balada; et.al., 2007).

Při kompetenci k podnikavosti by se měla rozvíjet žákova cílevědomost, zodpovědnost, tvořivost a kladný vztah k inovování. Žák objevuje svá nadání a uvědomuje si jejich využití v budoucím profesním životě. Umí prakticky využít získané dovednosti a znalosti. Při osvojení kompetence k podnikavosti je žák schopen kriticky zhodnotit výsledek své činnosti a na základě tohoto posouzení stanovit další potřebné kroky k dosažení stanovených cílů. (Balada; et.al., 2007).

1.3 Ekonomika a finance v RVP G

Téma „Ekonomika a finance“ v RVP G z roku 2007 je zařazeno v kapitole Člověk a svět práce. Tato vzdělávací oblast slouží k přípravě žáka na budoucí profesní a ekonomický život. Nastiňují se mu profesní i ekonomické situace, se kterými se v běžném životě setká. Proto je žák v této vzdělávací oblasti seznámen se základními ekonomickými pojmy, hospodářskými strukturami státu a vlivem globalizovaného světového trhu na světovou ekonomikou. Dále se učí o svých právech a pracovních povinnostech a hodnotí své pracovní dovednosti, které jsou nezbytné pro jeho profesní kariéru. Cílem vzdělávací oblasti Člověk a svět práce je, aby žák dokázal kriticky a analyticky přemýšlet nad aktuálním ekonomickým a pracovním trhem a zhodnotit jeho vlastnosti na základě svých teoretických znalostí. V této vzdělávací oblasti se ukazují různé modelové situace, které mají napomoci ke správnému aplikování získaných znalostí v běžném životě (Balada; et.al., 2007).

Kapitola Člověk a svět práce se skládá z podkapitol: Trh práce a profesní volba, Pracovněprávní vztahy, Tržní ekonomika, Národní hospodářství a úloha státu v ekonomice, Finance. Pro tuto bakalářskou práci jsou klíčovými podkapitolami: Tržní ekonomika a Finance (Balada; et.al. 2007).

1.4 Tržní ekonomika

RVP G očekává od hodin tržní ekonomiky tyto výstupy:

- Žák objasní mechanismy fungování trhu na základě konkrétní reálné situace. (Balada; et.al., 2007)
- Žák vyčísli cenu zboží a služeb, přičemž cenu stanoví jako součet nákladů, zisku a DPH. Vysvětlí vliv vývoje nabídky a poptávky na kolísání cen zboží a pracovní síly.
- Žák se nenechá manipulovat cenovými triky (cena bez DPH aj.) a klamavou nabídkou.
- Žák rozezná a porovná jednotlivé formy podnikání, přičemž je schopen odůvodnit, který typ podnikání je nejvhodnější ke konkrétní situaci.
- Žák zhodnotí klady a zápory podnikání ve srovnání se zaměstnáním. (Balada; et.al., 2007)

- Žák zná postup při zakládání vlastní podnikatelské činnosti a při žádosti o živnostenské oprávnění.
- Žák zaznamená skrytý obsah reklamy a kriticky zhodnotí podíl marketingu na úspěchu výrobku na trhu.(Balada; et.al., 2007)

Do učiva tržní ekonomiky řadí RVP G znalost témat:

- ***Základní ekonomické pojmy*** – typy ekonomik, ekonomický cyklus, tržní mechanismus, nabídka, poptávka, tvorba ceny, globální ekonomické otázky
- ***Ekonomické subjekty*** – právní formy podnikání (živnost, typy obchodních společností, družstvo), základní právní normy týkající se podnikání
- ***Marketing*** – marketing a public relations, reklama, reklamní agentury. (Balada; et.al., 2007)

1.5 Finance

RVP G očekává od hodin financí tyto výstupy:

- Žák je schopen využívat běžné platební nástroje a smění peníze za použití kurzovního lístku.
- Žák vysvětlí principy vývoje ceny akcií a vyjmenuje druhy investic do cenných papírů.
- Žák uvede rozdíl mezi pravidelnými a nepravidelnými příjmy a výdaji domácnosti, což mu bude sloužit jako podklad pro sestavení rozpočtu domácnosti.
- Žák předloží řešení schodkového rozpočtu a předloží návrhy smysluplného využití přebytkového rozpočtu domácnosti.
- Žák se orientuje v právech spotřebitele, což dokáže na příkladu jejich využití při nákupu zboží a služeb.
- Žák zhodnotí způsoby využití volných finančních prostředků (spoření, produkty se státním příspěvkem, cenné papíry, nemovitosti aj.)
- Žák si zvolí nejvýhodnější úvěrový produkt s ohledem na své potřeby a vysvětlí důvod svého rozhodnutí.

- Žák objasní metody stanovení úrokových sazeb a rozdíl mezi úrokovou sazbou a RPSN
- Žák si zvolí na základě svých požadavků nejvýhodnější pojistný produkt.
- Žák vysvětlí funkce ČNB a její pravomoci ovlivňující činnost komerčních bank.
- Žák ovládá využívání moderních forem bankovních služeb (Balada; et.al., 2007)

Do učiva financí řadí RVP G znalost témat:

- ***Peníze*** – funkce peněz, formy platebního styku v tuzemské i zahraniční měně, cenné papíry, akcie; burza.
- ***Hospodaření domácnosti*** – rozpočet domácnosti, typy rozpočtu a jejich rozdíly, tok peněz v domácnosti; spotřební výdaje, práva spotřebitele, předpisy na ochranu spotřebitele.
- ***Finanční produkty*** – způsoby využití přebytku finančních prostředků, spořicí a investiční produkty, další způsoby investování peněz; řešení nedostatku finančních prostředků, úvěrové produkty, leasing; úrokové sazby, RPSN; pojištění.
- ***Bankovní soustava*** – ČNB a komerční banky, specializované finanční instituce, moderní formy bankovnictví. (Balada; et.al., 2007)

1.6 ICT v RVP G

Tato oblast RVP G prohlubuje schopnosti žáků využívat digitální technologie. Klade důraz na použití komunikačních technologií, využívání důvěryhodných informačních zdrojů, chápání nových softwarových a hardwarových prvků digitálních technologií. (Balada; et.al., 2007).

Cílové zaměření vzdělávací oblasti Informatika a informační a komunikační technologie směřuje k utváření a rozvíjení klíčových kompetencí tím, že vede žáka k: porozumění základním pojmům a metodám informatiky jako vědního oboru; uplatňování algoritmického způsobu myšlení; využívání výpočetní techniky ke zvýšení efektivnosti své činnosti, ke znalosti způsobů prevence a ochrany před zneužitím a omezováním osobní svobody člověka; získávání údajů z většího počtu alternativních zdrojů

a odlišování informačních zdrojů věrohodných a kvalitních od nespolehlivých a nekvalitních; k respektování duševního vlastnictví, copyrightu, osobních dat a zásad správného citování autorských děl.

Kapitola Informatika a informační a komunikační technologie se skládá z podkapitol: Digitální technologie, Zdroje a vyhledávání informací, Komunikace, Zpracování a prezentace informací. Pro tuto bakalářskou práci jsou klíčovou podkapitolou Digitální technologie (Balada; et.al., 2007).

1.7 Digitální technologie v RVP G

RVP G očekává od hodin digitálních technologii tyto výstupy:

- Žák rozumí dostupným prostředkům ICT, dokáže je využívat a propojit.
- Žák spojuje teoretické i praktické poznatky o funkcích jednotlivých složek hardwaru a softwaru k tvůrčímu a efektivnímu řešení úloh.
- Žák účelně systematizuje data a chrání je proti poškození či zneužití.
- Žák uvede možnosti uplatnění ICT v různých oblastech společenského poznání a praxe. (Balada; et. al., 2007)

Do učiva financí řadí RVP G znalost témat:

- ***Informatika*** – vymezení teoretické a aplikované informatiky.
- ***Hardware*** – funkce prostředků ICT, jejich částí a periferií, technologické inovace, digitalizace a reprezentace dat.
- ***Software*** – funkce operačních systémů a programových aplikací, uživatelské prostředí.
- ***Informační sítě*** – typologie sítí, internet, síťové služby a protokoly, přenos dat.
- ***Digitální svět*** – digitální technologie a možnosti jejich využití v praxi.
- ***Údržba a ochrana dat*** – správa souborů a složek, komprese, antivirová ochrana, firewall, zálohování dat.
- ***Ergonomie, hygiena a bezpečnost práce s ICT*** – ochrana zdraví, možnosti využití prostředků ICT handicapovanými osobami. (Balada; et. al., 2007)

2 Peníze

Definovat tento pojem by se mohlo zdát snadné, avšak opak je pravdou. Jedná se o neurčitý a proměnlivý pojem založený na důvěře. Do poloviny minulého století tomu tak nebylo. Veškeré bankovky existovaly formou úpisu, který mohl vlastník vyměnit za své zlato uchované u bankéře. Dnes jsou to uměle vytvořené jednotky, které jsou respektovány společností. Jejich primárním účelem je zjednodušení směnného procesu, který nebyl vždy tak jednoduchý jako dnes (Cervenka, 2014).

Tvorba peněz je dnes jednoduchá. Schválené množství je zadáno do systému a potvrzeno autoritou národní banky. Nově vzniklý elektronický obnos je zapůjčen ostatním bankovním společnostem. Banky však téměř vše použijí ke své činnosti kromě malého množství určeného jako rezerva. Rezerva se liší podle legislativy státu, ve kterém se banka nachází. Teoreticky pak banky tyto peníze zmnoží. Dochází k tomu skrze půjčky banky od ostatních bankovních společností spolu s NB. Peníze, které banka půjčuje, ve své podstatě nemá, ale vytvoří je na základě dluhu. V literatuře je uvedeno, že banky mohou půjčit desetinásobek rezervy. (Cervenka, 2014).

Nejdůležitějšími vlastnostmi peněz jsou hodnota, zaměnitelnost, skladovatelnost a dělitelnost. První zmíněnou vlastností je hodnota peněz, která se v průběhu času měnila, protože dříve se hodnota mince určovala více parametry jako je například váha nebo složení. V dnešní době je důležité, aby peníze byly zaměnitelné, to znamená, že hodnota nezáleží na vnějších parametrech, ale na nominální hodnotě. Kvůli zefektivnění a zjednodušení platebního procesu musí peníze splňovat nároky na skladovatelnost a mobilitu. Peníze proto musí být volně k dispozici s odpovídajícími rozměry pro směnu a uchovávání. V rámci zachování obchodovatelnosti peněz je dalším kritériem jejich dělitelnost. Dělitelností je myšlena jako možnost rozměnit peníze na menší součásti, díky kterým je vyrovnán rozdíl hodnoty mezi jednotlivým zbožím. Proto je výhodnější při koupi zlata preferovat malé slitky před nakoupením celého prutu (Rothbard, 2001; Starr, 1989).

Peníze se na základě své historie staly prostředkem směny, měřítkem ceny, uchovatelem hodnoty a v některých případech i měřitelem vykonané práce. Jako první funkce je uváděna platební funkce, která zjednodušuje proces směny. Díky vytvoření platebních mechanismů, které jsou právně prokazatelné, je možné pomocí peněz platit. Směna i cena dále závisí na depozitní funkci peněz, která umožňuje kapitál uchovávat v podobě vkladů,

čímž dochází k akumulaci prostředků. Kvůli likviditě je možné převádět finanční prostředky na hotovost. Díky investicím lze uchovat hodnotu peněz v dané komoditě, čímž je zachována kupní síla investora. Od hodnoty peněz se odvíjí i cena jednotlivých komodit a služeb, které jsou hodnoceny a ceněny pomocí peněz (Rothbard, 2001; Starr, 1989).

2.1 Historie peněz

Vznik a vývoj peněz jde ruku v ruce s vývojem společnosti. S narůstající potřebou usnadnit tzv. „směnný obchod“. Směnný obchod fungoval na principu výměny zboží za zboží. Tento typ obchodu měl mnoho nevýhod. Největší nevýhodou bylo velmi složité oceňování zboží a následně samotná směna, která byla značně komplikovaná (Bertl, 2018; Cervenka, 2014; Juřík, 2012).

Problém s tímto složitým směňovacím systémem byl vyřešen našimi předky zavedením prvních platidel, kterými byly mušle, pírka, kusy plátna nebo pálené destičky. Tyto první alternativy však byly postupem času nahrazeny drahými kovy. První mince, podobné dnešním, byly vytvořeny již v 7. století př. n. l. na území tehdejší Malé Asie (dnešní Turecko). Jednalo se o slitky stříbra a zlata, které se nazývaly „statéry“. I přesto, že mince pomohly lidem ocenit dané zboží a značně ulehčily proces směny, byly stále považovány za nepraktické kvůli jejich velké váze a špatnému skladování. Z toho důvodu v 9. století vznikaly v Číně první papírové bankovky. V Evropě se první papírové bankovky začínaly používat až v 17. století (Bertl, 2018; Juřík, 2012).

V dnešní době se mince nebo bankovky používají méně, protože je dávána přednost bezkontaktním platbám. To znamená, že peníze vlastník nedrží fyzicky u sebe. Zaměstnavatel zašle peníze na účet zaměstnance, ten následně platí kartou nebo tyto peníze využije při platbách na internetu (Cervenka, 2014; Juřík, 2012).

Platební karty se vyvinuly z „věrnostních karet“, které vznikly u obchodníků v USA koncem 19. století a fungovaly na principu předplaceného kreditu, který byl zapsán do knihy a následně jím mohl zákazník platit. Nemusel s sebou nosit peníze. Nicméně tento systém byl náročný na administrativu, proto společnosti přišly s papírovou platební kartou, která fungovala na podobném principu, jenže tuto papírovou kartu měl zákazník u sebe. První platební karta, jak ji známe, vznikla roku 1948. Byla vytvořena společností „Air Travel Card“, která touto kartou chtěla ulehčit obchodování zákazníků v letecké dopravě (Juřík, 2012).

2.2 Historie bankovnictví

Mezi úplně první bankovní operace, které byly prováděny, by bylo možné zařadit lichvářství prováděné mocnými rodinami v Itálii na přelomu třináctého a čtrnáctého století našeho letopočtu. Následně se z těchto praktik objevily první náznaky bank a bankovního systému vedeného právě členy zmíněných rodin. Veškeré transakce byly zapisovány do účetních knih a pod dohledem církve se z těchto zřízení staly opravdové bankovní společnosti. Italský bankovní systém se v šestnáctém století našeho letopočtu stal modelem bankovnictví v Evropě.

Začátkem sedmnáctého století v Amsterdamu vznikla první banka zabývající se směňováním měn. Touto dobou také vznikala možnost převodu peněz mezi účty bez fyzického vyzvednutí peněz. V polovině sedmnáctého století se začaly objevovat banky, které půjčovaly více, než umožňovala jejich zásoba peněz, jedná se o významný krok k dnešnímu bankovnictví. Třetím významným milníkem sedmnáctého století se stala možnost převést dluh státu na akcie, které byly volně prodejné. V osmnáctém století hrály banky velkou roli při industrializaci celé Evropy díky usnadnění platebních machinací mezi jednotlivými společnostmi.

Začátkem devatenáctého století dostává Anglická národní banka status centrální národní banky a s ním právo na kontrolu anglických peněz. V polovině devatenáctého století vzniká v Anglii první zákon o lichvě v Evropě, čímž došlo k omezení úrokové sazby. Díky příznivým podmínkám začaly být bankovní služby dostupnější širšímu množství klientů. Vyvstává otázka týkající se velikosti rezervy finančního obnosu uchovávaného v bankách. Kvůli zachování schopnosti vyplatit klientům množství financí, které potřebovali, byly banky nuceny vydělávat peníze skrze obchod s akciemi velkých společností. Na začátku dvacátého století došlo ke stabilizaci systému díky rozmachu spořících oddělení bank, které poskytovaly klientům možnost ukládat a hodnotit své peníze prostřednictvím bank, což poskytlo bankovním společnostem dostatečnou rezervu financí.

V polovině dvacátého století došlo k úpadku mnoha nestabilních bankovních společností a tím k protřídění trhu a ustálení konkurence. V sedmdesátých letech dvacátého století byla ve Spojených státech amerických zrušena možnost směnit své peníze za zlato jejich hodnoty. Došlo tedy k odkrytí měny, která je nyní přijímána na základě veřejné důvěry (Ferguson, 2011).

2.3 Banky, bankovní systém, digitální a virtuální měny

Největší výhodou a zároveň nevýhodou bank je jejich centralizovaný systém. Tato výhoda umožňuje klientům efektivní a bezpečné využívání bezhotovostních plateb. Klient se nestará o osud svých peněz v bance, věří, že pokud bude platit kartou nebo přes internet, bude mít peníze k dispozici. Banka je prostředník mezi klienty, a proto nenastávají problémy mezi zákazníky a obchodníkem. Banka jako centrální autorita řeší převod financí za své klienty (Bertl, 2018; Cervenka, 2014; Revenda, 2012).

Banky tuto službu neposkytují bezplatně. Většina bank vydělává na poplatcích a na tom, že půjčuje peníze svých klientů jiným klientům. Tímto způsobem banka vydělává. Většině zákazníků tento způsob hospodaření s penězi nevadí a akceptují tento postup, protože jsou rádi, že mohou využívat služeb banky (Bertl, 2018; Cervenka, 2014; Švarcová, 2013).

Tento způsob vydělávání peněz vznikl již při vzniku bankovek, kdy lidé nosili drahé kovy k tehdejšímu bankéřovi, který jejich drahé kovy schoval a dal jim bankovku, která potvrzovala, že on u sebe uchovává drahé kovy v hodnotě této bankovky. Následně bankéři začali půjčovat peníze a začali vypisovat bankovky, které nebyly kryté drahými kovy. Tento systém může fungovat za předpokladu, že máme velké množství klientů, kteří si nevybírají své peníze a banka může s jejich penězi nakládat podle vlastní potřeby (Ferguson, 2011; Švarcová, 2013).

Příkladem selhání celého bankovního systému může být krize v roce 2007. Krizi předcházelo nekontrolované schvalování půjček spolu s nekontrolovaným nákupem cenných papírů. Následně došlo ke zhroucení systému, kdy zadlužení klienti nebyli schopni splácet. Téměř došlo ke krachu mnoha velkých bankovních společností (Vebler, 2018).

V aktuálním světě je velice těžké si představit hospodaření se svými penězi bez prostřednictví bank kvůli tomu, že je většina plateb digitálních. Žádný jednotlivec nemá možnost si v bankovním systému založit svoji digitální peněženku, kterou by si spravoval sám. Bylo by zde totiž riziko, že jednotlivec začne podvádět a připisovat si více peněz do své digitální peněženky (Bertl, 2018; Švarcová, 2013).

Fiat měna

Fiat měnou se myslí forma peněz státu nebo seskupení státu, které vytvořily jednotnou měnu. Je definována měnovým zákonem daného uskupení. Za její vydávání, hodnotu i kurz zodpovídá nadřazený orgán nebo instituce (Revenda, 2012).

Digitální měna

Tímto pojmem se myslí finanční prostředky převedené do digitální formy, které jsou uznávány jako forma reálné měny. Prostřednictvím prostředníka dochází k převodu peněz do elektronické podoby. Příkladem mohou být peníze na běžném bankovním účtu, které jsou v dnešní době uchovávány v elektronické podobě (Vebler, 2018; Schlossberger, 2012).

Virtuální měna

Jedná se o neregulované virtuální platidlo, které je spravováno a distribuováno výhradně mezi členy speciální online komunity. Nejčastěji se virtuální měna získává směnou za reálné peníze. Zpětně nelze tyto tokeny směňovat za existující měnu. Druhým způsobem je provádět specifickou činnost v daném virtuálním prostředí (European Central Bank, 2012).

Virtuální měna se dělí na měnu s uzavřeným, redukovaným a neredukovaným tokem.

Uzavřená měna funguje pouze v daném prostředí. Jedná se například o herní měny, kdy hráč nakoupí komoditu za vlastní peníze a dále může s měnou fungovat pouze ve hře, kde tyto peníze získal. Příkladem můžou být *RP body* hry *League of Legends*, kdy hráč za nakoupené body může nakupovat bonusové herní prvky (European Central Bank 2012).

Měna s regulovaným tokem může být směňována za reálné služby nebo zboží. Většinou je nakoupena přímo za reálné peníze a nelze ji zpětně vyměnit. Jedná se například o *Nintendo body,* za které může být nakoupen software od společnosti *Nintendo* (European Central Bank, 2012).

Měna s neredukovaným tokem se blíží kryptoaktivu. Po nakoupení lze směnit zpět za reálnou měnu. Má vlastní kurz a hodnotu v daném virtuálním prostředí, proto lze používat pro nákup služeb a zboží. Jako příklad lze brát *LindeDolars* z virtuálního světa *Second Life* (European Central Bank, 2012).

3 Kryptoaktiva

Jedná se o obchodovatelná virtuální aktiva zabezpečená pomocí kryptografie, která brání před double spending problémem. Operace s nimi nejsou označovány jako platební metoda. Tyto kryptoaktiva jsou často decentralizované sítě založené na technologii blockchainu. Převod jednotlivých kryptoaktiv probíhá pseudoanonymně skrze zakódované algoritmy ve formě hashů s asymetrickým šifrováním. První kryptoaktivum vzniklo roku 2009, kdy Satoshi Nakamoto vytvořil genesis block bitcoinu. V nynější době je prezentováno nepřeberné množství kryptoměn (Bertl, 2018; Stroukal; et. al., 2018; Frankenfield, 2020; Vebler, 2018; Nakamoto, 2008).

3.1 Důležité pojmy

51% útok

Při zařazení nového bloku do blockchainu dojde k ověření pravdivosti zbytkem sítě skrze ověření nonce. Pokud by útočníci docílili ovládnutí více než 50 % sítě, mohli by schvalovat bloky, které by do blockchainu za normálních okolností nemohly být přiřazeny. Mohlo by tedy docházet k double spending problému. Jediným řešením vzniklé dominance by se stalo odříznutí nepravdivých bloků pomocí tvrdé vidlice (Blockbase Mining, 2020; Stroukal; et. al., 2018).

ASIC

ASIC je zkratka z anglického „Application Specific Integrated Circuit“, neboli „Integrovaný obvod pro konkrétní aplikaci“. Zkratkou ASIC se označuje speciální typ zařízení, které je sestaveno primárně na dělání pouze jedné činnosti, například těžba kryptoaktiv je na ASIC zařízení mnohonásobně efektivnější než těžba za pomocí procesorů, či grafických karet (Narayanan; et. al., 2016).

ASIC resistence

Jedná se o ochranu při těžbě kryptoaktiva proti ASIC zařízením. Princip této ochrany spočívá v navýšení požadavků na RAM počítače. Jedná se například o hybridní algoritmus Lyra2rev2. Tyto resistence se používají kvůli tomu, aby se do sítě těžařů mohli připojit i těžaři, kteří nevlastní ASIC zařízení (Narayanan; et. al., 2016).

Těžba na ASIC zařízení je natolik efektivní, že kryptoaktiva bez ASIC resistence se bez ASIC zařízení nevyplatí těžit (Narayanan; et. al., 2016).

Blockchain

Je otevřená databáze, která funguje na principu distribuování všech dat mezi všechny uživatele, a tato data se ukládají do řetězce bloků. Bloky obsahují informace o předchozím bloku ve formě jeho hashe. Bloky v sobě mají informaci o provedených transakcích kryptoaktiv, o čase na vytvoření bloku a o těžaři, který tento blok vytvořil. Kvůli zaheslované informaci předchozího bloku – hashi – na sebe bloky navazují (tvoří řetězec), není možné měnit předchozí bloky, a tím pádem ani historii transakcí (Stroukal; et. al., 2018; Eyal; et. al., 2014).

Kdokoliv může získat kopii kompletního blockchainu. Kvůli tomu je síť neustále udržována kompletní a bez vnějšího zásahu. Pokud by se objevil chybný nebo padělaný blok, uživatelé blockchainu by změnu zaznamenali a chybné bloky by byly odstraněny (Stroukal; et. al., 2018; Eyal; et. al., 2014).

Block reward

Je odměna těžaři za přidání bloků do blockchainu. Odměna za blok je obvykle pevná, ale některá kryptoaktiva, jako je například bitcoin, snižují svoji odměnu po uplynutí určitého času. Jedná se o způsob, kterým jsou kryptoaktiva distribuovány těžařům za spravování sítě. (Narayanan; et. al., 2016; Stroukal; et. al., 2018; Eyal; et. al., 2014).

Block size

Je velikost bloku, která je omezena počtem bitů (Narayanan; et. al., 2016; Stroukal; et. al., 2018).

Block time

Je průměrná doba vytěžení jednoho bloku. Block time se používá k zabezpečení sítě a kontroly náročnosti těžení. Pokud je zapotřebí k rozšifrování algoritmu více času než obvykle, dojde ke snížení náročnosti algoritmu. Pokud je příliš krátká prodleva mezi uzavřenými bloky, je obtížnost kódu zvýšena. Náročností algoritmu se myslí složitost hashe, který má být vyprodukován. Block time ovlivňuje mnoho faktorů, avšak tím největším je počet těžařů (Narayanan; et. al., 2016).

Circulating supply

Je množství mincí v oběhu. Tento počet nezohledňuje ztracené mince a mince na „mrtvých“ peněženkách – to jsou takové peněženky, na kterých nebyla delší dobu provedena žádná transakce, jejich majitel pravděpodobně zapomněl přístupové údaje do

peněženky, proto se tyto mince již nikdy nedostanou do oběhu. Circulating supply je ukazatel počtu mincí, které již byly vytěženy (Stroukal; et. al., 2018).

Dapps

Jsou to decentralizované aplikace bez centrální autority založené na principu blockchainu, kdy obsah není uložen na centrálním serveru, ale je distribuován mezi uživatele skrze uzly. Příkladem může být DTube, což je decentralizovaná platforma pro sdílení videí. Neexistuje centrální autorita, protože pravidla užívání a obsah jsou v rukou uživatelů (Blockgeeks, 2019).

Double spending problem

Jedná se o typ útoku na síť kryptoaktiva, kdy útočník použije jeden obnos mincí pro vícero transakcí (pošle stejných 100 mincí na vícero peněženek). Mohl by nastat například při 51% útoku. V bankovním systému tento problém řeší banka, která na proces jako centrální autorita dohlíží. Má-li klient na účtu 100 Kč, nemůže deseti svým kamarádům poslat 100 Kč, protože banka eviduje jeho peníze. Při 51% útoku by si útočník mohl potvrzovat transakce a tím pádem opětovně poslat kryptoaktiva, která již poslal někomu jinému (Stroukal; et. al., 2018).

General ledger

General ledger funguje jako průběžná účetní kniha, která umožňuje retrospektivně nahlížet do již uzavřených bloků. Transakce v blockchainové síti fungují na matematicky stejném principu jako bankovní transakce, k jednomu účtu se přičítá a od druhého se odčítá. Pokud chceme zjistit aktuální stav uzlu, podíváme se pomocí general ledgeru do bloku, který v tomto uzlu naposledy uzavíral transakci. Díky general ledgeru není potřeba průběžně uchovávat informace o všech uzlech, ale pouze o těch, na kterých proběhla změna (Narayanan; et. al., 2016).

Genesis block

Jedná se o nultý blok, který je prvním blokem v blockchainu. Tento blok je výjimečný, protože obsahuje počáteční transakci a je zakódovaný do softwaru (Eyal; et. al., 2014; Nakamoto, 2008).

GPU

Jedná se o grafické karty, pokročilejší verze CPU, které vznikly kvůli vykreslování obrazu ve videohrách či videích. Výhodou CPU karet byla zvýšená kapacita operací díky

velkému počtu jader procesorů. GPU jsou grafické karty zaměřené na těžbu kryptoaktiv, proto je oproti CPU počet jader navýšen. Při těžení kryptoaktiv je prováděno opakované dosazování nonce k informacím bloku, proto více operací na kartách GPU zaručuje vyšší efektivitu (Klein, 2020).

Hash

K jeho získání používáme hashovací funkci, což je matematický algoritmus, který se používá v databázích, na internetu a v kryptografii. Při použití hashovací funkce dojde k zašifrování dat do jednoduchého zkráceného kódu obsahující směs číslic, písmen a znaků. Informace zakódované v hashi se dají rozkódovat pomocí private key (Narayanan; et. al., 2016; Eyal; et. al., 2014; Shirriff, 2019).

Hash rate

Je to míra výpočetní obtížnosti, kterou těžař potřebuje, aby zvládl uzavřít blok. Vypočítá se jako počet terahashů za vteřinu (Blockchain.com, 2020).

Lightning network

Jedná se o druhou vrstvu sítě pohybující se nad Bitcoinem. Touto sítí je řešen problém s rychlostí převodu Bitcoinu, kdy příjemce platby má jistotu, že platba proběhla až poté, co jsou informace o ní zapsány do bloku. Dochází k otevření kanálu přístupného na základě klíče pouze pro účastníky platby. Je vytvořena adresa kanálu nazývající se multisig, na kterou jedna strana nahraje aktiva a druhá je vyzvedne. Platba tedy proběhne, ale k převodu dojde až při zapsání do bloku. Druhá strana však má jistotu, že aktiva obdrží. Pokud si druhá strana aktiva nevyzvedne, nejsou ztracena, ale odesílatel má možnost stáhnout je z adresy multisigu (Stroukal; et. al., 2018).

Miner´s fee

Je poplatek uživatele těžaři. Jedná se o malou část přidanou k transakci, která má těžaře povzbudit ke zpracování transakcí a přidat je do dalšího bloku. Velikost bloku je omezená počtem transakcí, které mohou být v každém bloku zprostředkovány, proto uživatelé mohou ovlivnit velikost tohoto poplatku, aby byla jejich transakce zapsána do aktuálního bloku (Blockbase Mining, 2020).

Mining pool

Zakladatel prvního poolu – „Slush pool“, je Čech Marek Palatinus, který je také zakladatel hardwarové peněženky trezor. Jedná se o skupinové těžení, kvůli zvýšení

pravděpodobnosti vytěžení nového bloku. Pokud pool vytěží blok nějakého kryptoaktiva a získá odměnu, je tato odměna rozdělena mezi všechny členy podle procent. Tato procenta jsou rozdělena podle poměru výpočetní síly jednotlivých uživatelů, která byla vynaložena k vytěžení bloku. Aktuálně zaujímá „Slush pool“ 4 % všech těžařských poolů na světě (Palatinus, 2020; Rubario, 2020).

Nodes

Nodes neboli uzel, je počítač, který je součástí sítě. V krypto světě máme tři typy uzlů, kdy každý z nich má odlišnou úlohu v síti. Prvním typem je světlý uzel, který je schopen validovat kopii blockchainu. Dále může přijímat a vytvářet transakce, proto je někdy nazýván jako peněženka. Druhým typem je plný uzel, který v sobě má uloženou celou kopii blockchainu, je důležitý pro chod celé sítě, nicméně ne vždy za ni má člen plného uzlu odměnu. A posledním typem je těžařský uzel, na kterém těžaři přidávají transakce do blockchainu a vytvářejí tak nové bloky (Blockbase Mining, 2020).

Nonce

Náhodné číslo, které těžař hledá tak, aby po dosazení do hashovací funkce bloku vyšel hash s co největším počtem nul na začátku přepisu (Blockbase Mining, 2020).

Proof of work

Je důkaz prací, bez tohoto principu by si jednotliví činitelé sítě nedůvěřovali. Pokud chce těžař uzavřít bloky, musí nejprve dešifrovat hash. Za svoji odvedenou práci získá odměnu v podobě daného kryptoaktiva. Tato aktiva jsou potvrzením, že k jejich vzniku byl zapotřebí výpočetní výkon a energie (Blockbase Mining, 2020; Nakamoto, 2008).

Public key / private key

Jedná se o formu asymetrického kryptografického šifrování, kdy šifrování a dešifrování probíhá podle jiných klíčů, které se navzájem nedají odvodit. Tato metoda umožňuje odeslat zašifrované informace veřejného klíče tak, aby příjemce mohl dešifrovat informace pouze pomocí soukromého klíče. Příkladem použití může být elektronický podpis, kterým těžař podepíše a zašifruje sebou vytvořený blok. Skrze vlastní soukromý klíč mohou všichni vidět informace v bloku i podpis (Stroukal; et. al., 2018).

Smart contract

Tyto kontrakty jsou naprogramovatelnou funkcí blockchainu. Jedná se o virtuální alternativy smluvních podmínek. Fungují na principu dohody dvou subjektů na

domluvených podmínkách plateb. Pokud jsou podmínky kontraktu splněny, daná platba proběhne (Blockgeeks, 2019).

Těžba

Je proces, při kterém je pomocí výpočetního úkonu dosazována nonce do bloku tak, aby při následném „zhashování“ celého objemu dat vyšel z procesu hash s nižší hodnotou, než je systémem požadováno. Náročnost pro uzavření bloku se mění v závislosti na hash rate. Pokud hash bloku nesplňuje parametry, je do celé funkce zadána nová nonce (Stroukal; et. al., 2018; Nakamoto, 2008; Shirriff, 2019).

Total supply

Je celkové množství kryptoaktiv, které bude vytvořeno v dané síti. Těžením se vytváří nová kryptoaktiva. Tento proces není nekonečný. Většina kryptoaktiv má již předem stanovený počet, kolik jich bude vytvořeno. V budoucnu nastane situace, že se bloková odměna zastaví a těžaři budou odměňováni pouze poplatky za transakci (Blockbase Mining, 2020).

Vidlice blockchainu

Jedná se o rozdělení řetězce bloků, ke kterému dojde při úpravě nebo změně vlastností blockchainu. Dělí se na měkké a tvrdé vidlice. Měkké vidlice umožní pokračovat ve starém blockchainu. Tvrdé vidlice okamžitě znemožní přidávat bloky na starou větev (Narayanan; et. al., 2016; Eyal; et. al., 2014).

Wallet address

Peněženky jsou softwarové aplikace, které ukládají public key a private key umožňující uživatelům interakci s jejich kryptoaktivy. Adresa krypto peněženky je generována z hashovaného veřejného klíče pomocí algoritmu P2PKH. Za pomocí public key může vlastník přijímat transakce, za pomocí private key je může posílat.(Sedgwick, 2002)

3.2 Blockchain

Jedná se o řetězec zakódovaných souborů – bloků – s datovým obsahem o dané kapacitě úložného prostoru a vlastním protokolem. Makroskopicky ho lze chápat jako navazující seznam postupně zapisovaných dat, na který lze připojovat aplikace. Celý systém nespadá pod jednu centrální organizaci, je tedy decentralizovaný. Je otevřený a tím i dostupný k nahlížení. (Stroukal; et. al., 2018; Eyal; et. al., 2014).

Jednou z jeho nejdůležitějších vlastností je neměnitelnost. I přes to, že není kontrolován centrální buňkou je blockchain vytvořen tak, že každý nově vytvořený blok obsahuje hash předchozího bloku. Pokud by proto byla změněna informace v jednom bloku, neodpovídala by informace žádného z následujících a chybný blok by byl nahrazen opět původním blokem. Systém je tedy velmi bezpečný, málo náchylný ke kyberútokům a stabilní, neměnný. (Stroukal; et. al., 2018; Eyal; et. al., 2014).

Dalším parametrem blockchainu je distribuce celé databáze do uzlů. Každé zařízení, které s blockchainem operuje, se stává uzlem sítě a vlastní tak kopii celého řetězce. Dochází tak k úpravám, kontrolám správnosti i přidávání nových bloků. Všechny uzly v síti jsou pseudoanonymní, tzn., že nelze vystopovat reálnou identitu vlastníka. (Stroukal; et. al., 2018; Eyal; et. al., 2014).

Blockchain také nikdo nevlastní a o chod celého systému se starají jeho uživatelé. Tento mechanismus se nazývá P2P. Uzly, které přidávají informace do bloků za spotřebovanou energii, dostávají odměnu ve formě kryptoaktiva sítě, kterou spravují. (Stroukal; et. al., 2018; Eyal; et. al., 2014).

Hlavním obsahem informace uložené v blockchainu jsou transakce kryptoaktiv. V dnešní době se však objevují teorie, že tento systém je budoucností veškeré infrastruktury.

Celý tento systém se tedy řídí vlastním protokolem. Blockchainový protokol definuje uspořádání systému a udává jeho parametry, jako jsou například podmínky nonce nebo velikost souborů ukládaných do bloků. Tento základ systému může být pozměňován a upravován pomocí vidlic nebo cíleným upravením parametrů. (Stroukal; et. al., 2018; Eyal; et. al., 2014).

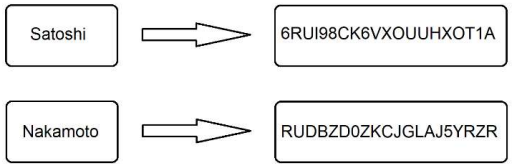
Kódování jednotlivých bloků je řešeno tzv. asymetrickým šifrováním. Jedná se o typ šifrování, ve kterém se liší klíče pro šifrování a dešifrování souborů. Privátní klíč je vygenerován pro každého uživatele a z něho je vytvořen klíč veřejný, který jsou schopni získat všichni uživatelé sítě. V praxi to poté probíhá tak, že privátním klíčem je schopen uživatel operovat se svým účtem/peněženkou, díky veřejnému klíči zase ostatní uživatelé vědí, že je to právě ten jeden uživatel. Transakce jsou následně kódovány oběma klíči a po rozšifrování podpisu je ověřeno, že transakce opravdu proběhla a byla schválena odesílatelem. Pro toto asymetrické šifrování je používána hashovací funkce. Ta je rychlá, bezpečná, jednosměrná, dobře čitelná a identifikovatelná. (Stroukal; et. al., 2018; Eyal; et. al., 2014).

3.3 Šifrování dat v blockchainu

Šifrování dat v blockchainové síti probíhá pomocí hashovacího algoritmu. Tento algoritmus šifruje vstupní data a převádí je do jednoho unikátního řetězce znaků – hash. Tento způsob šifrování dat je jednosměrný, to znamená, že z hashe nejdou získat vstupní data.

Nezávislé hashování

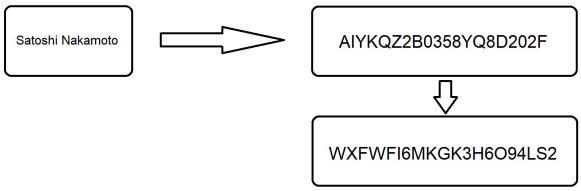
Nezávislé hashování šifruje všechna data jednotlivě.



Obr. 2: Hashování – nezávislé – vlastní tvorba

Opakované hashování

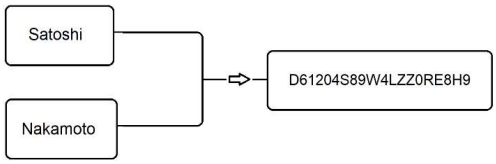
Opakované hashování zašifruje vstupní data, která následně opět zašifruje.



Obr. 3: Hashování – opakované – vlastní tvorba

Kombinované hashování

Kombinované hashování šifruje více vstupních dat dohromady. Ze vstupních dat vznikne pouze jeden hash.



Obr. 4: Hashování – kombinované – vlastní tvorba

3.4 Využití blockchainu

Témata blockchain a kryptoaktiva jsou spojovány především se světem financí, kdy se uživatelé snaží za pomocí těchto technologií vytvořit nový prostředek směny bez centrální autority. Nicméně problém centrálních autorit mají i jiná odvětví, a proto i u nich se objevuje myšlenka blockchainu (Hřivna, 2018).

Pojišťovnictví

Aplikování blockchainu do sektoru pojišťovnictví by přineslo pro tento obor mnoho výhod: automatizace, digitalizace, úsporu papírových dokumentů nebo zjednodušení plateb pojistného (Hřivna, 2018).

Blockchain by zde mohl sloužit jako společná databáze pojistných smluv a pojištěných předmětů, mohl by být propojený s policií a jinými subjekty, které by do sítě mohly přidávat data (Hřivna, 2018).

Pojišťovnictví na systému blockchain by fungovalo tak, že lidem by bylo vypočítáno pojistné, kterým by pravidelně přispívali do sítě. Tento příspěvek by nebyl zisk pojišťovny, ale tvořil by finanční rezervu dané sítě. Z této rezervy by se pak vyplácely peníze v případě pojistné události. Kvůli použití chytrých kontraktů by byla síť do velké míry plně automatizovaná. O schválení pojistné události by namísto pojišťovny rozhodovali uživatelé. Tím by se usnadnilo vyplácení pojistného plnění, protože to by bylo vypláceno ze společné rezervy. V tomto systému by mohla fungovat zaštiťující autorita, která by zaštiťovala pojistnou síť pro případ, že by došla společná finanční rezerva. Za tuto správu by si zajišťovací autorita mohla brát poplatek ze společné rezervy (Hřivna, 2018).

Příklad takového modelu, může být decentralizovaná aplikace Teambrella, která funguje na platformě Ethereum (Paperno, 2017).

Zdravotnictví

Ve zdravotnictví by blockchainová síť vedla k usnadnění dokumentace mezi lékaři a klienty. Usnadnila by se tak komunikace mezi lékařem a pacientem. Zpřehlednila by se historie operací, očkování, výsledků testů a tento systém by mohl být také propojen se zasíláním informací na pojišťovnu. Další výhodou by bylo usnadnění byrokracie, při které by nedocházelo k duplikaci dokumentů (Hřivna, 2018).

Klient by ke sdílení těchto informací uděloval povolení, to by mohlo probíhat pomocí privátního klíče, který by tato data dočasně zpřístupnil (Hřivna, 2018).

Aplikace, která se touto problematikou již zaobírá, je MedRec. Jedná se o aplikaci blockchainu Etherea. V této aplikaci musí existovat autorita, která spravuje přidávání informací do sítě (Hřivna, 2018).

Logistika

Blockchain by za pomocí chytrých kontraktů mohl v logistice pomoci s digitalizací dokumentů, rychlostí zpracování objednávek, kontrole zboží a automatizaci plateb mezi jednotlivými subjekty (dodavateli). Zavedení blockchainu v logistice by také vedlo k synchronizování způsobu uchovávání dat. V dnešní době používají subjekty v logistice různé systémy uchovávání dat, což často vede ke zbytečně časově náročnému převádění jednotlivých dat. V této synchronizaci by za pomocí chytrých kontraktů mohla probíhat automatizace účetních knih (Hřivna, 2018).

K tématu logistiky patří i otázka zboží. Lidé v dnešní době se více zajímají o původ potravin a zboží, proto by jejich evidence v blockchainové databázi mohla přinést dostupný přehled důležitých informací. Myšlenkou uchovávání dat zboží se zabývá společnost Project Provenance Ltd, která si klade za cíl vytvořit platformu, na které by zákazníci pomocí čárového, nebo QR kódu mohli zjistit časové razítko, informace o výrobci, informace o produktu či jiné užitečné údaje. Tato data by byla uložena na blockchainové databázi. Pravdivost informací má být ověřována odbornými audity, na jejichž základu by byly informace vkládány do blockchainu (Baker, 2013).

Project Provenance Ltd by tuto databázi chtěl udělat dostupnou na mobilní zařízení, aby si každý zákazník mohl zkontrolovat složení produktu a zdali výrobce ve firmě neporušuje lidská práva (Baker, 2013).

Energetika

V dnešním světě si někteří lidé instalují solární panely a jiná zařízení na výrobu vlastní elektrické energie. Tato energie se dá dále distribuovat, avšak v dnešní době je to velmi problematický proces. Pokud by se elektrická síť napojila na blockchain, usnadnil by se obchod mezi poskytovateli a odběrateli elektrické energie. Na tomto blockchainu by si odběratelé mohli vybrat svého poskytovatele dle vlastních priorit. V této síti by bylo vše za pomocí chytrých kontraktů automatizované, proto by nebyl zapotřebí prostředník, který by tento obchod zprostředkoval (Hřivna, 2018).

Tento způsob distribuce elektrické energie by přinesl výhodu poskytovatelům, kteří by se mohli snadno zbavovat své elektrické energie. Tato síť by byla plně transparentní a nemohlo by v ní, kvůli uchovávání dat v blockchainu, docházet k milným informacím, takže by každý odběratel zaplatil přesně tolik, kolik spotřeboval. Vznik takovéto distribuce elektrické energie by mohl řešit problémy v oblastech, kde je komplikované připojení na hlavní elektrickou síť (Hřivna, 2018).

Aplikace Exergy se snaží o vytvoření této sítě (Pando LO3energy, 2018).

3.5 Vlastnosti kryptoaktiv

Vlastnosti jednotlivých kryptoaktiv a jejich využití se mezi sebou často liší. Stále vznikají nová kryptoaktiva, která se snaží získat uživatele novými funkcemi. Uživatel si v dnešní době může vybrat z mnoha kryptoaktiv na základě různých preferencí. Z toho důvodu většina uživatelů používá více různých kryptoaktiv.

Cena

Pro cenu kryptoaktiv je důležitý proof of work neboli PoW, dokázání praxí. Jedná se o podložení kryptoaktiva reálnou prací. Jako byly peníze kryté zlatem, kryptoaktiva jsou krytá spotřebovanou energií, která je nezbytná k jejich vytěžení. Těžař neprodává vytěžené kryptoaktivum za nižší cenu než jsou jeho náklady k vytěžení. Tato vlastnost je důležitá k správnému ohodnocení kryptoaktiva (Narayanan; et. al., 2016; Bertl, 2018; Kaliský, 2018).

Decentralizace

Mnoho uživatelů kryptoaktiv nevěří ve spolehlivost bank a jiných finančních institucí, které mají plnou kontrolu nad jejich finančními toky. Tyto centralizované systémy jsou nebezpečné, protože dotyčná instituce může s klientovými penězi jakkoliv nakládat bez vědomí klienta. Pokud je kryptoaktivum decentralizované, má vlastník plnou kontrolu nad svými prostředky a nehrozí například zpronevěra peněz nebo zamrazení účtu. Žádný jednotlivec nebo skupina nemůže nezávisle na ostatních ovlivnit vlastnosti kryptoaktiva (Narayanan; et. al., 2016; Bertl, 2018; Fillner, 2014).

Peer to peer

Peer to peer neboli P2P, rovný s rovným, tímto způsobem mezi sebou jednotlivé subjekty v „kryptosvětě“ obchodují. Jedná se o posílání transakcí bez prostředníka. Na rozdíl od bankovní společnosti, která kontroluje pohyb klientových peněz a v některých případech

vyžaduje i poplatek za provedenou transakci. Peer to peer vlastnost vznikla kvůli tomu, aby se zjednodušily transakce mezi uživateli (Bertl, 2018; Kaliský, 2018; Nakamoto, 2008).

Pseudoanonymita

V bankovním systému mají banky přehled o všech klientových nákupech a transakcích. To znamená, že jsou schopny zjistit, kdy, kde a kdo nakupoval, kolik utratil a co nakoupil. Transakce v blockchainové síti jsou pseudoanonymní, protože probíhají mezi jednotlivými peněženkami, které neobsahují osobní údaje. To znamená, že lze zpětně dohledat, kdy proběhla transakce, jaké množství aktiva bylo převedeno i informace o obou peněženkách. Anonymita spočívá v ochraně údajů vlastníka peněženky, které skrze systém nelze dohledat (Narayanan; et. al., 2016; Bertl, 2018; Stroukal; et. al., 2018; Fillner, 2014).

Celosvětové použití

Při transakci aktiv nezáleží na poloze, vzdálenosti ani státní příslušnosti. Pohyb mezi peněženkami je závislý pouze na připojení k internetu a aktivitě těžařů. Kdyby byla kryptoaktiva používána jako klasická platidla, byl by usnadněn mezinárodní obchod, protože by nebyla zapotřebí směna jedné měny za druhou (Bertl, 2018; Fillner, 2014).

Průhlednost systému

Díky blockchainovému uspořádání sítě jsou veškeré operace kryptoaktiva dohledatelné. Nemůže tedy dojít k zpětným úpravám systému. Neustále dochází k porovnávání správnosti celého blockchainu, na kterém se podílí velké množství uzlů (Narayanan; et. al., 2016; Shirriff, 2019).

Zodpovědnost

Jelikož je síť kryptoaktiv spravována bez prostředníka, v bankovním světě se jedná o bankovní společnost, jsou uživatelé nabádáni k obezřetnosti. Pokud je chyba ve vlastním zadání transakce, těžař ji zadá do bloku a již není možné zadání změnit. Pokud by proto bylo odesláno nesprávné množství kryptoaktiv nebo by se vyskytla chyba v adrese peněženky, nebylo by možné ztracené aktivum získat zpět (Stroukal; et. al., 2018; Nakamoto, 2008).

3.6 Historie kryptoaktiv

Za zakladatele kryptoaktiv a zároveň nejrozšířenějšího kryptoaktiva Bitcoinu je považován člověk, nebo skupina lidí, která vystupuje pod pseudonymem Satoshi Nakamoto. Tento člověk (případně skupina) zveřejnil 31. 10. 2008 dokument „Bitcoin: A Peer-to-Peer Electronic Cash System“. Tento dokument popisuje principy fungování Bitcoinu (Stroukal; et. al., 2018; Nakamoto, 2008).

Klíčové datum v historii Bitcoinu je 3. 1. 2009. V tento den vytěžil Satoshi Nakamoto genesis block, jedná se o nultý blok. Tento den si většina nadšenců připomíná tím, že stáhnou svá kryptoaktiva z burz. Jedná se také o ověření, že burza neobchoduje s neexistujícími kryptoaktivy a neumožňuje lidem obchodovat s aktivy, které nevlastní. Tímto se snaží uživatelé předejít problému, který lze pozorovat u bank. Pokud si klient vloží své peníze do banky, banka zpravidla dál investuje nebo půjčuje jeho finance. Klient toto chování bank v běžném životě nepocítí. Problém by nastal v moment, kdyby si všichni klienti banky chtěli vybrat své peníze a banka by tyto peníze neměla (Kaliský, 2018; Javůrek, 2018).

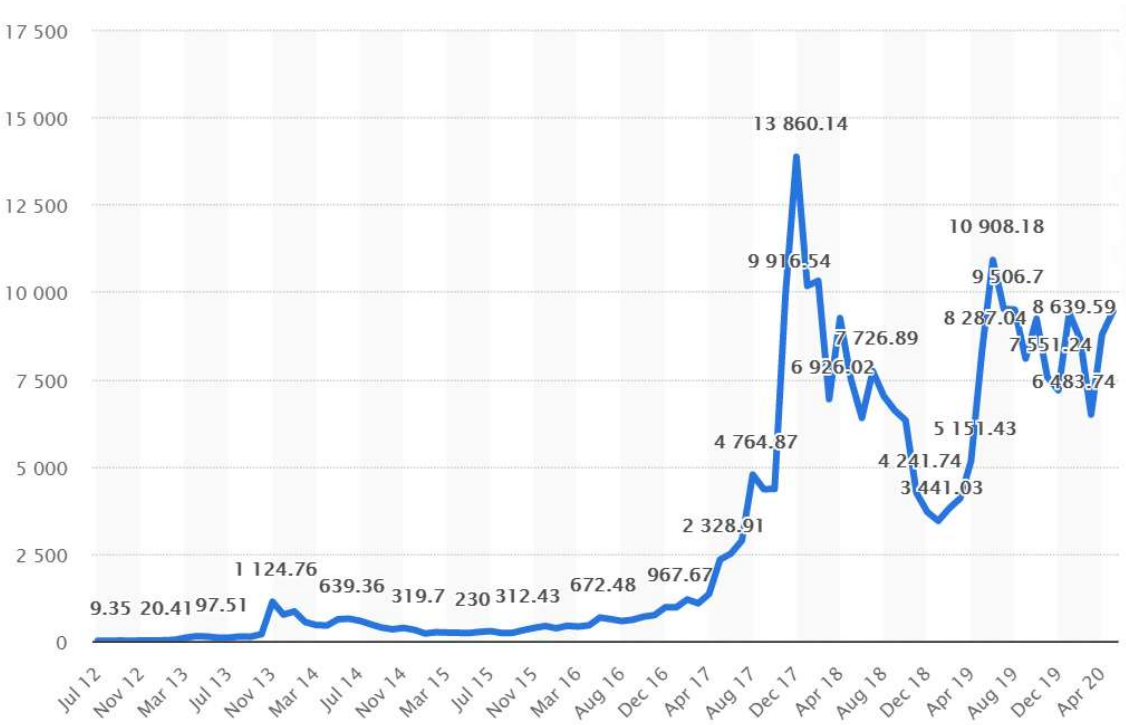
Dne 22. 11. 2009 vzniklo Bitcointalk (Bitcointalk, 2009) fórum, které založil zakladatel Bitcoinu Satoshi Nakamoto. Toto fórum vzniklo, aby se na něm sdružovali krypto nadšenci. Bitcointalk není fórum zaměřené pouze na Bitcoin, avšak řeší se zde i ostatní kryptoaktiva. Bitcointalk fórum je aktivní i v roce 2020 (Bitcointalk, 2009).

V roce 2010 se Bitcoin začíná objevovat na prvních burzách. Jednou z největších byla Mt.Gox (Mt.Gox, 2018). Tato burza také obchodovala s online variantou karetní hry Magic: The Gathering. Tuto burzu nechvalně proslavil hackerský útok v roce 2014. Hackeři ukradli 850 000 bitcoinu, které měly v tu dobu hodnotu 450 000 000 dolarů. Burze Mt.Gox se podařilo 200 000 bitcoinů získat zpátky, nicméně většina okradených, kteří obchodovali na této burze, nezískali kompenzaci své ztráty (Mt.Gox, 2018).

Před otevřením burz se cena 1 bitcoin obchodovala za 0,008 $. Krátce po otevření burz se vyšplhala cena bitcoinu na 0,08 $. Koncem roku 2012 vznikla první oficiální burza Paymium (Paymium, 2020).

Rok 2013 můžeme označit za zlomový. Cena jednotky bitcoinu stoupá až k 1151 $. V tomto roce se kryptoaktiva dostávají více do masových médií, nicméně tento trend

utichá v roce 2014 kvůli výraznému poklesu ceny bitcoinu (Paymium, 2020).



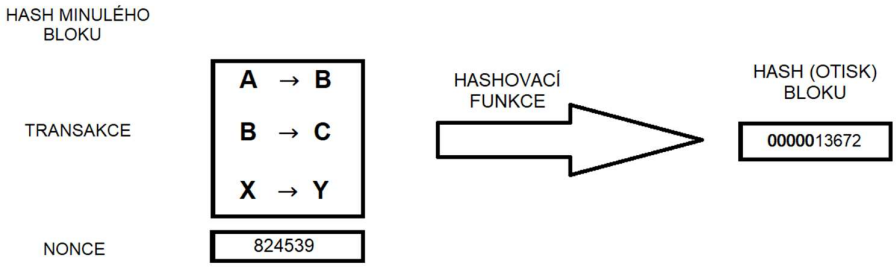
Graf 1: Vývoj ceny bitcoinu v letech 2012 až 2020 (Rudden, 2020)

3.7 Těžba kryptoaktiv

Vysvětlení technického principu těžby kryptoaktiv

Těžbou kryptoaktiv se nazývá uzavírání blocků v blockchainu. Těžař používá hash minulého bloku kvůli návaznosti blockchainu, následně přidá informace o transakcích, které proběhly od doby uzavření předchozího bloku a nakonec zkouší přidávat k bloku různé nonce. Následně na tento soubor informací aplikuje hashovací funkci a pozoruje vypočítaný hash. Pokud je výsledek nižší, než požaduje aktuální obtížnost těžení závislá na hash rate, je nový blok uzavřen (Stroukal; et. al., 2018; Kaliský 2018; Nakamoto, 2008; Shirriff, 2019).

Rychlost těžby záleží na block time. Pokud se těžařům daří rychle uzavírat bloky, stane se algoritmus složitějším, respektive bude chtít hash s více nulami na začátku. V momentě, kdy těžař najde funkční nonci, může uzavřít blok. Nicméně před uzavřením ještě zbylí těžaři vyzkouší tuto nonci, aby se přesvědčili, že je tato nonce správná. Tímto způsobem se kryptoaktiva chrání před podváděním od těžařů (Stroukal; et. al., 2018; Nakamoto, 2008; Shirriff, 2019).



Obr. 5: Hashování funkce – těžba kryptoaktiv – vlastní tvorba

3.8 Historie těžby

Způsoby těžby kryptoaktiv se neustále vyvíjejí a těžaři se tímto způsobem snaží získat výhodu před ostatními. Této výhody lze docílit dvěma způsoby. První ze způsobů je mít levnější elektřinu než ostatní těžaři, čímž je docíleno vyššího zisku z vytěžených kryptoaktiv. Druhý způsob je těžit na zařízení s výkonnější výpočetní technologií (Stroukal; et. al., 2018; Nakamoto, 2008; Shirriff, 2019).

Těžba na procesorech

V samých počátcích kryptoaktiv se dala všechny kryptoaktiva těžit pomocí CPU procesorů. Stačilo stáhnout software. Tyto procesory mají pouze jednotky jader, takže čtyřjádrový CPU procesor zvládal pouze čtyři hashovací funkce současně, což bylo neefektivní (Stroukal; et. al., 2018; Nakamoto, 2008; Shirriff, 2019).

Těžba na grafických kartách

Kvůli zvýšené poptávce po kryptoaktivech přemýšleli těžaři, jak vylepšit způsob těžení. Začali těžit na grafických kartách GPU. Tyto grafické karty měly výhodu v počtu jader, které se pohybují v jednotkách tisíců. Na rychlejší těžbu se používá tzv. RIG, což je počítač s více grafickými kartami (Stroukal; et. al., 2018; Nakamoto, 2008; Shirriff, 2019; Bohemiasoft, 2017)).

ASIC

ASIC je zkratka z anglického „*Application Specific Integrated Circuit*“, neboli „Integrovaný obvod pro konkrétní aplikaci“. Těžba na tomto zařízení je v dnešní době

nejefektivnější, například bitcoin se bez zařízení ASIC nevyplatí těžit kvůli vysoké konkurenci a rychlosti, s jakou ASIC zařízení provádí operace (Narayanan; et. al., 2016).

3.9 Peněženka kryptoaktiv

Jak kryptoaktiva získávají oblibu ve světě, ruku v ruce s tím jde i jejich pokrok, který je často iniciován z řad uživatelů různých kryptoaktiv. I přesto, že se jedná o virtuální peníze, které nemají fyzickou podobu, tak i pro kryptoaktiva vznikají hmatatelné peněženky, které si kladou za cíl udržet kryptoaktiva v bezpečí (Narayanan; et. al., 2016; Stroukal; et. al., 2018; FINEX, 2020).

Softwarová peněženka

Jedná se o program, který si uživatel stáhne do počítače. Tento program vygeneruje peněženku, na které může ukládat svá kryptoaktiva. Jedná se o jednu z nejstarších metod uchovávání kryptoaktiv. Tento způsob ukládání aktiv je bezpečný podle toho, nakolik je v bezpečí počítač v online i offline světě. Jeden z příkladů takovéto peněženky je program MultiBit (Narayanan; et. al., 2016; Stroukal; et. al., 2018).

Online peněženka

Tento způsob uchování aktiv spočívá v jejich umístění na onlinové burzy, například coinbase. Toto je velmi nebezpečný způsob uschování kryptoaktiv, protože burza může být napadena hackrem. Jako například v roce 2014, kdy byla vykradena burza Mt.Gox. Jedinou výhodou, kterou online peněženky mají, je jejich uživatelské rozhraní, které umožňuje uživatelům snadno a rychle hospodařit s kryptoaktivy (FINEX, 2020).

Mobilní peněženka

Jak již název napovídá, jsou určeny pro smartphony. Tyto peněženky jsou bezpečnější než online peněženky a jsou určeny především pro uživatele, kteří kryptoaktiva používají na každodenní bázi, anebo se s nimi teprve učí zacházet. Jednou z mobilních peněženek je například XWallet, která je ke stažení na Google Play (Stroukal; et. al., 2018; FINEX, 2020).

Papírová peněženka

Jedná se o vygenerovaný, vytisknutý public key a private key. Největší nevýhodou tohoto typu peněženek je jejich jednoduchá ztráta nebo poškození. Papírové peněženky jsou však snadno uschovatelné a nelze je ukrást v online světě (Narayanan; et. al., 2016; Stroukal; et. al., 2018).

Hardwarová peněženka

Hardwarové peněženky svým majitelům neumožňují flexibilní zacházení s kryptoaktivy. Jejich držitel však má jistotu, že jsou jeho kryptoaktiva v bezpečí. Na trhu s hardwarovými peněženky dominují dvě firmy – Trezor a Ledger. První zmíněná hardwarová peněženka byla vynalezena v České republice (Stroukal; et. al., 2018).

Hardwarová peněženka po své vizuální stránce připomíná flash disk. Při jejím aktivizování získá majitel seed, což je speciální kód složený z 12, 18 nebo 24 slov. Tento seed slouží jako „pojistka“ proti ztracení. (Stroukal; et. al., 2018; Palatinus, 2020).

3.10 Seznam nejpoužívanějších kryptoaktiv

Rozdíl mezi kryptoaktivy a altcoiny je ten, že pojmem altcoiny se označují kryptoaktiva bez bitcoinu. Altcoiny získaly toto označení kvůli jejich menší popularitě.

Bitcoin

Bitcoin je považovaný za první kryptoaktivum na světě. Za jeho vznikem na rozdíl od ostatních kryptoaktiv stojí anonymní tvůrce nebo tvůrci, kteří na internetu vystupují pod pseudonymem Satoshi Nakamoto. Bitcoin funguje na principu proof of work. Tento princip fungování je nyní ve velké oblibě uživatelů, někteří vytváří svá vlastní kryptoaktiva, která do velké míry kopírují bitcoin (Stroukal; et. al., 2018; Eyal; et. al., 2014; Kaliský, 2018; Javůrek, 2018; Nakamoto, 2008; Shirriff, 2019).

Stejně jako všechny kryptoaktiva, která fungují na principu blockchainu, tak i bitcoin uzavírá bloky. Algoritmus je nastaven tak, aby průměrný block time byl 10 minut. Total supply bitcoinu je 21 milionů mincí a nikdy jich nebude víc (Stroukal; et. al., 2018; Eyal; et. al., 2014; Javůrek, 2018; Nakamoto, 2008; Shirriff, 2019).

Litecoin

Jedná se o jeden z nejstarších a nejstabilnějších altcoinů. Byl založen dne 5. 10. 2011 a jeho zakladatel je Charlie Lee, bývalý zaměstnanec Googlu. Jedná se o rychlejší alternativu bitcoinu (Stroukal; et. al., 2018; Lee, 2011).

V roce 2014 prohlásil o litecoinu jeho zakladatel Charlie Lee, že je litecoin již hotový a nebudou na něm probíhat žádné další úpravy. Kvůli tomuto prohlášení se litecoin až do začátku roku 2017 nevyšplhal cenou nad 4 $. V roce 2017 se na litecoinu opět zahájila práce. Druhý největší rozmach litecoinu nastal v roce 2018, kdy se jeho cena pohybovala

okolo 400 $. Jeho zakladatel kvůli střetu zájmu nyní nevlastní žádný litecoin (Stroukal; et. al., 2018; Lee, 2011).

Litecoin se od bitcoinu liší především v parametrech. Jeden z těchto parametrů je total supply čítající 84 milionů litecoinu. Další rozdíl oproti bitcoinu je v průměrném block timu, který je nastaven na 150 sekund, tím pádem jsou transakce v této síti rychlejší (Stroukal; et. al., 2018; Lee, 2011).

Ethereum

Je název celého projektu, obchoduje se s jednotkou ETH. Zakladatel tohoto projektu je Vitalik Buterin, který pochází z Ruska, avšak od svých 6 let žije v Kanadě. Vitalik Buterin se poprvé s bitcoinem setkal ve svých 17 letech, kdy obdržel nabídku napsat o bitcoinu článek na blog, odměnou za tento článek mělo být 5 BTC. Vitalik Buterin se začal více zajímat o bitcoin a blockchain, napadaly ho projekty, které by se daly na principech bitcoinového blockchainu vystavět, avšak setkával se s odporem bitcoinové komunity, pro kterou je prioritou bezpečnost a tyto nové technologie by ji mohly ohrozit, proto koncem roku 2013 představil projekt Ethereum. Cílem tohoto projektu je vytvořit decentralizovaný systém, na kterém by fungovaly decentralizované aplikace. Tyto aplikace by fungovaly na etherovém blockchainu a spravovali by je sami uživatelé. Jeden ETH se skládá z 1 000 000 000 000 000 000 wei (Bohemiasoft, 2017; Buterin, 2013).

Czech Crown coin

Jedná se o českou alternativu Litecoinu, která byla vytvořena Ladislavem Faithem. Používá algoritmus script a díky tomu lze těžit pomocí normálních počítačů i technologie ASIC. Část měny byla před zpřístupněním aktiva předtěžena. Tento vytěžený obnos měl být rozdělen mezi občany ČR. V dnešní době se aktivum nepoužívá (Bořánek, 2014; Sassen, 2017).

Tether

Tether je takzvaný stablecoin. Tímto pojmem se označuje kryptoaktivum, jehož cena je shodná s cenou některé fiat měny. Tether vznikl za účelem ulehčení směny mezi USD a kryptoaktivy, protože některé burzy, na kterých se obchodují kryptoaktiva, odmítají přijímat fiat měnu. Tether není vázaný na klasický bankovní systém, za jeho správou stojí společnost Tether Limited (Tether Limited, 2018).

Tether funguje na principu „Proof of Reserves“, neboli důkaz rezervou, který funguje tak, že daná společnost kryje dotyčné kryptoaktivum reálnými finančními prostředky. Ty jsou kontrolovány průběžnými audity, které mají za cíl zkontrolovat, zdali dotyčná společnost nedistribuuje kryptoaktiva ve větší hodnotě, než kolik je schopna pokrýt (Tether Limited, 2018).

Ohledně Tetheru a společnosti Tether Limited existují spekulace, že nejsou schopny finančně pokrýt počet mincí v síti. Pokud by byla spekulace pravdivá, vedla by tato situace k poklesu ceny všech kryptoaktiv, protože Tether je jedním z kryptoaktiv (Tether Limited, 2018).

Cardano

Cardano se snaží o vytvoření lepšího blockchainu, chce urychlit přenos dat pomocí side chainy, což jsou sekundární boční řetězce sítě a tzv. shardingem, což je rozdělování blockchainu na menší části. Vývojáři tohoto altcoinu do své sítě implementují systém hlasování, snaží se tím předejít k nespokojenosti uživatelů a hard forkům. Mnoho kryptoaktiv má problém s financování vývoje, nebo se spoléhá na práci dobrovolníků. Cardano tento problém řeší pomocí tzv. treasury, což je odkládání části nově vytěžených mincí do společné pokladny, o které pomocí systému hlasování rozhodují uživatelé (Hoskinson, 2015).

Hlavním vývojářem a propagátorem cardana je Charles Hoskinson (Hoskinson, 2015).

4 Didaktika

4.1 Metody vyučování

Vyučování je považováno za jedno z nejdůležitějších didaktických kategorií, jelikož tvoří základ systematického výchovně-vzdělávacího procesu, který komplexně rozvíjí osobnost člověka, zejména tedy dítěte a mladého člověka. Vyučování chápané jako institucionalizovaná forma výchovy je celistvý systém, jehož prvky (učitel, žák, prostředí, vyučovací metody a prostředky…) jsou vnitřně spjaty a ve svém celku představují koncepci vyučování. Společenské, vědní a estetické poznání v sobě odráží reálnou výchovu podobně jako vyučování.(Mazáčová, 2014).

Učitel na žáka působí prostřednictvím výchovných a výukových metod. Těžiště výchovných metod tkví v rodině, zatímco škola se na pozadí výchovných metod soustředí především na ty výukové. Mezi ony výchovné metody patří přesvědčování, vzor, příkazy, pravidla, hodnocení, ocenění, tresty, pomoc, spolupráce, hraní rolí, dramatizace a inscenace (Jůva, 1983). Nicméně tato bakalářská práce se bude věnovat především výukovým metodám. Autorem jedné z nejrozšířenějších definic výukové metody je Josef Maňák, který ji popisuje jako uspořádaný systém činností učitele a aktivit žáka, jež vedou k dosahování výchovně-vzdělávacích cílů.(Maňák, 2003).

Komunikace mezi učitelem a žákem probíhá prostřednictvím činností žáka, jenž se učí a jeho učitele, který ho vyučuje. Z výše uvedeného vyplývá, že učitel žákům zprostředkovává nejen osvojení si potřebných vědomostí a dovedností, ale i návyků. Učitel by měl ke každému žáku přistupovat individuálně, vnímat jeho specifické předpoklady k učení, jeho schopnosti a jeho míru samostatnosti a tvořivosti. Každý učitel musí zvolit takové vyučovací metody, které budou přiměřené rozumové, tělesné a emocionální vyspělosti žáků. (Maňák, 2001)

Základ tradiční výukové metody představovala činnost učitele, jenž vystupoval v roli organizátora činnosti žáků. Novější výukové metody zdůrazňují především samostatnou aktivitu žáků, která formuje jejich vlastní styl učiva. Na výběr vhodné výukové metody má nezanedbatelný vliv vztah mezi učitelem a žákem. Ke zdařilému výchovně-vzdělávacímu působení je nezbytná úzká spolupráce a podpůrné přátelské prostředí. Mezi hlavní funkce výukových metod patří zprostředkování vědomostí a dovedností, komunikační funkce a aktivizační funkce, která umožňuje rozvíjet žákovo myšlení. (Maňák, 2001).

4.2 Průběh modelových hodin

Před začátkem vyučovací hodiny přicházím do třídy, abych si připravil potřebné pomůcky k výuce a představil se žákům. Žáky, kteří vstupují do třídy, zdravím a využívám čas na tvorbu vztahu. Využívám neformální situace před začátkem hodiny, bavím se studenty na téma: „Co Vás ve škole baví, jaký je Váš oblíbený předmět, kam chcete na vysokou?“

V momentě, kdy má začínat výuka, požádám žáky o ticho a čekám, dokud se třída neztiší. Pokud se třída neztiší, požádám znovu žáky o ticho. Při ztišování třídy jsem trpělivý. Jakmile nastane ticho, tak ho nechám chvilku působit. V prvních 5 minutách se snažím naladit na třídu, je-li unavená, jsem energetický, je-li hlučná, jsem tichý. (Junior Achievement, 2000; Krpálek; et. al., 2012)

Na začátku vyučování se představím žákům a seznámím žáky s průběhem vyučovací hodiny. Téma hodiny se snažím zkombinovat se znalostmi, které si již osvojili. Vysvětlím žákům, v čem je dané téma pro ně důležité a jak ho využijí v běžném životě. (Junior Achievement, 2000; Krpálek; et. al., 2012)

Během průběhu hodiny dodržuji základní pravidla pro správné vedení hodiny: Pohybuji se po místnosti (nezůstávám při výkladu na jednom místě), nemluvím déle než 5 minut v kuse, při výkladu používám příklady z praxe, do hodiny se snažím zapojit všechny žáky, opakovaně si ověřuji, že žáci pochopili výklad, pracuji s intonací hlasu a tempem řeči, se žáky udržuji oční kontakt. (Junior Achievement, 2000; Krpálek; et. al., 2012)

Čas	**Fáze vyučovací jednotky**
3 min	**Úvod, organizace**
2 min	**Motivace –** představení nového učiva a jeho význam
7 min	**Opakování předcházejícího učiva -** formou ústního zkoušení, her, otázek,…
15 min	**Výklad nového učiva**
12 min	**Upevňování probraného učiva –** odstranění nejasností, samostatná práce žáků
4 min	**Shrnutí –** ověření zvládnutí nového učiva
2 min	**Rozdání dotazníků, zhodnocení vyučovací hodiny**

Tab. 1: Harmonogram vyučovací hodiny (Krpálek; et. al., 2012)

Praktická část

5 Návrhy modelových hodin informatiky

5.1 Struktura první hodiny informatiky

Název: Využití algoritmů k zabezpečení informací – programování Caesarovy šifry

Charakteristika hodiny: Hodina je zaměřena na praktické pochopení a vyzkoušení Caesarova algoritmu. V první části hodiny si žáci zopakují pojmy z minulé hodiny včetně praktické úlohy na barevnost grafu. V druhé části hodiny žáci programují Caesarovu šifru v Excelu. Žák si během lekce procvičí logické myšlení a využití algoritmů během programování.

Klíčová slova: algoritmus, Caesarova šifra, barevnost grafu, Excel

Délka hodiny: 45 minut

Kontext hodiny: Hodina bude probíhat ve třídě druhého ročníku čtyřletého gymnázia nebo v sextě osmiletého gymnázia. Očekávaný věk žáků je 16-17 let. Tato hodina spadá v RVP G do kapitoly Informační a komunikační technologie a do podkapitoly Zpracování a prezentace informací, téma: Algoritmizace úloh. Optimální počet žáků na vyučovací hodině je dvacet čtyři. Od žáků je očekávána částečně odborná znalost tématu z předchozí vyučovací hodiny.

Touto vyučovací hodinou pokračujeme v tematickém plánu (Algoritmizace úloh). Na tuto hodinu by měla navazovat testovací hodina, která by měla zahrnovat test na téma: Grafové algoritmy, ve zbytku hodiny bude probírána těžba kryptoaktiv (bitcoinu).

Pomůcky:

- Tabule
- Projektor
- Křída nebo fix
- Sešit a psací potřeby
- Předpřipravené úlohy na procvičení barevnosti grafů

Cíle hodiny:

- Žák naprogramuje Caesarovu šifru v textovém programu Excel

Klíčové kompetence:

- Kompetence k učení
- Sociální a personální kompetence
- Kompetence k řešení problémů

Hodnocení: Při hodině je hodnocena spolupráce žáků s vyučujícím a aktivní zapojení žáků v samostatné činnosti. Hodnocení je slovní.

Uchování informací: Žáci dostanou pracovní list na zopakování barevnosti grafu a během hodiny naprogramují vlastní program. Žákům je umožněno zapisovat si poznámky a důležité informace do sešitů.

Časový harmonogram:

Časové rozmezí [min]	**Aktivita**
0–3	Úvod hodiny, seznámení žáků s průběhem hodiny
3–5	Motivace žáků k informatice
5–13	Zopakování pojmů z předchozí hodiny a praktické procvičení barevnosti grafů
13–17	Vysvětlení Caesarovy šifry
17–38	Programování Caesarovy šifry
38–43	Shrnutí hodiny – opakování grafových algoritmů, programování Caesarovy šifry
43–45	Rozdání dotazníků, zhodnocení vyučovací hodiny

Tab. 2: Hodina ICT 1 – vlastní tvorba

Popis aktivit:

Před začátkem hodiny

Vejdu do třídy a vítám příchozí žáky, abych je podpořil v dobrém zvyku chodit v čas. Tento čas před začátkem hodiny investuji do tvorby vztahu mezi mnou a žáky. Zajímám se o jejich názor a směji se jejich vtipům.

0–3 Úvod hodiny, seznámení žáků s průběhem hodiny

Poprosím žáky o ztišení. Představím se a dám prostor žákům, aby se mě doptaly na otázky, které je o mě zajímají. Seznámím žáky s průběhem hodiny: „Dneska si zopakujeme grafové algoritmy z minulé hodiny a naprogramujeme si jednoduché šifrovací tabulky v Excelu."

3–5 Motivace žáků k informatice

Začnu se žáky diskusi: „Mají pro Vás hodiny informatiky nějakou hodnotu? Učíte se na hodinách informatiky něco nového? Co byste se chtěli učit na hodinách informatiky?" Cílem této diskuse je namotivovat žáky ke studiu informatiky.

5–13 Zopakování pojmů z předchozí hodiny a praktické procvičení barevnosti grafů

„Minulou hodinu jsme probírali grafové algoritmy, je Vám vše, co jsme si řekli na minulé hodině, jasné?" Pokud budou mít žáci dotazy, tak na ně reaguji a zodpovím je.

„Co si pamatujete z minulé hodiny?" Dávám žákům prostor se vyjádřit. „V minulé hodině jsme se zabývali pojmy z grafových algoritmů a barevností grafů, tady jsem Vám připravil jeden graf na procvičení." Rozdám pracovní listy a dávám žákům prostor k řešení úlohy, mezitím obkreslím graf na tabuli. Jakmile vidím, že žáci dokončují cvičení, dám žákům prostor jít vyřešit tuto úlohu na tabuli. „Chcete někdo ukázat své řešení na tabuli, za plusko?" Žákovi, který se přihlásí rychle, zkontroluji výsledek, abych ho vyvaroval chybě. Cílem této aktivity je v dotyčném žákovi, který jde napsat řešení na tabuli, vyvolat pocit sebejistoty. Žák za svoji aktivitu získá plusko a pochvalu. „Máte nějaké dotazy ke grafovým algoritmům a barevnosti grafů?" Pokud se přihlásí žák, že tomu nerozumí, vysvětlím mu postup řešení této úlohy znovu. Při tomto vysvětlování nebudu používat moc odborných termínů, abych zvýšil šanci, že daný žák pochopí princip řešení barevnosti grafu. „Tímto jsme si zopakovali minulou hodinu, tak se můžeme posunout dál."

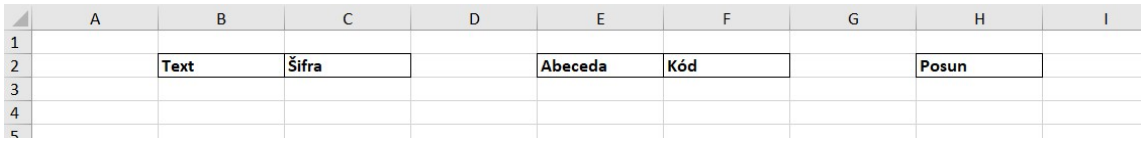
13–17 Vysvětlení Caesarovy šifry

Poprosím žáky, aby si zapnuli počítače. „Slyšeli jste pojem Caesarova šifra?" Pokud některý žák o Caesarově šifře již slyšel, nechám ho ji vysvětlit a případně ho doplním.

„Tuto šifru používal Julius Caesar při korespondenci během války, aby nepřítel, který zajal Caesarova posla, nezjistil, co píše. Caesarova šifra spočívá v tom, že každé písmeno abecedy zapisujete znakem jiného písmena. Aby se v tom odesílatel a příjemce vyznali, domluví si počet písmen, o kolik budou znaky posouvat. Pokud by si domluvili například posun o 1 písmeno, tak by se A zapisovalo jako B, B jako C, C jako D. Caesar používal posun o 3 písmena, takže A bylo D, B bylo E, C bylo F. Chápeme princip Caesarovy šifry?“ Pokud má žák dotaz, tak mu na něj odpovím.

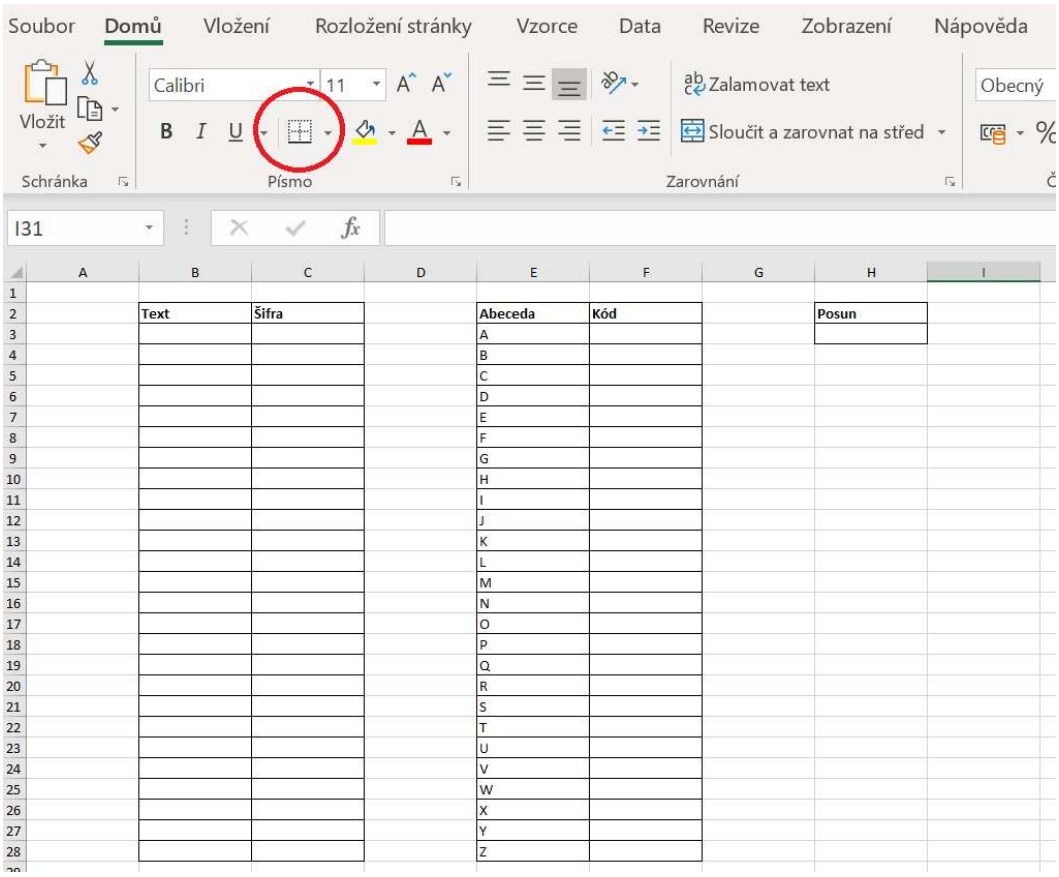
17–38 Programování Caesarovy šifry

Zapnu projektor, abych mohl jednotlivé kroky programování demonstrovat. „Teď si naprogramujeme šifrovací tabulku v Excelu. Proto si prosím zapněte Excel. Během tohoto programování budeme používat dvě funkce POSUN a SVYHLEDAT, pokud máte Excel v angličtině, budou to funkce OFFSET a VLOOKUP. Začneme tím, že si vytvoříme názvy klíčových sloupců tabulky, pojmenujeme si je: Text, Šifra, Abeceda, Kód a Posun. Později budeme do řádku Text psát zprávu, kterou chceme zašifrovat. Tato výsledná šifra se nám ukáže ve sloupci Šifra. Sloupce Abeceda a Kód budeme používat k přepisu jednotlivých písmen. Poslední sloupec Posun bude sloužit k tomu, abychom jsme si mohli určovat, o kolik znaky písmen posuneme. “



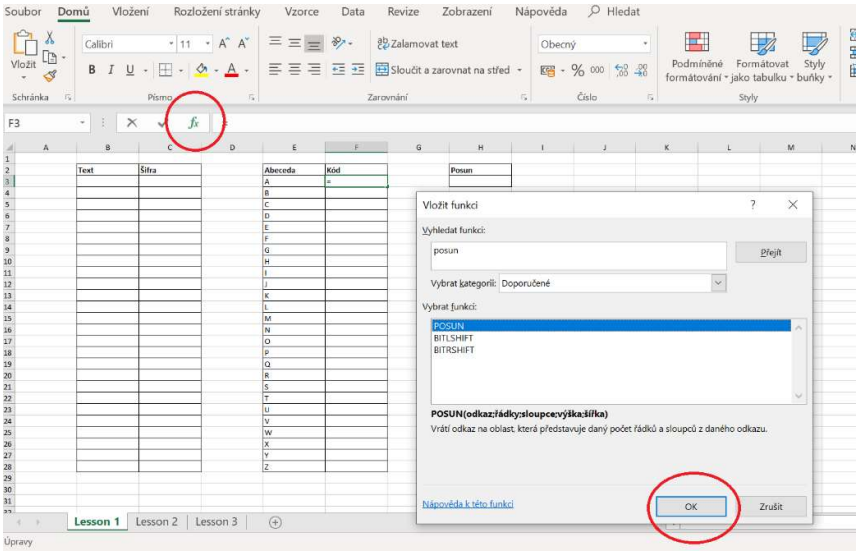
Obr. 6: Caesarova šifra krok 1 - vlastní tvorba

Pokud toto máte, vypište si prosím do sloupce Abeceda všechny znaky abecedy. Pokud chcete, můžete si důležité sloupce zvýraznit pomocí ohraničení buňky.



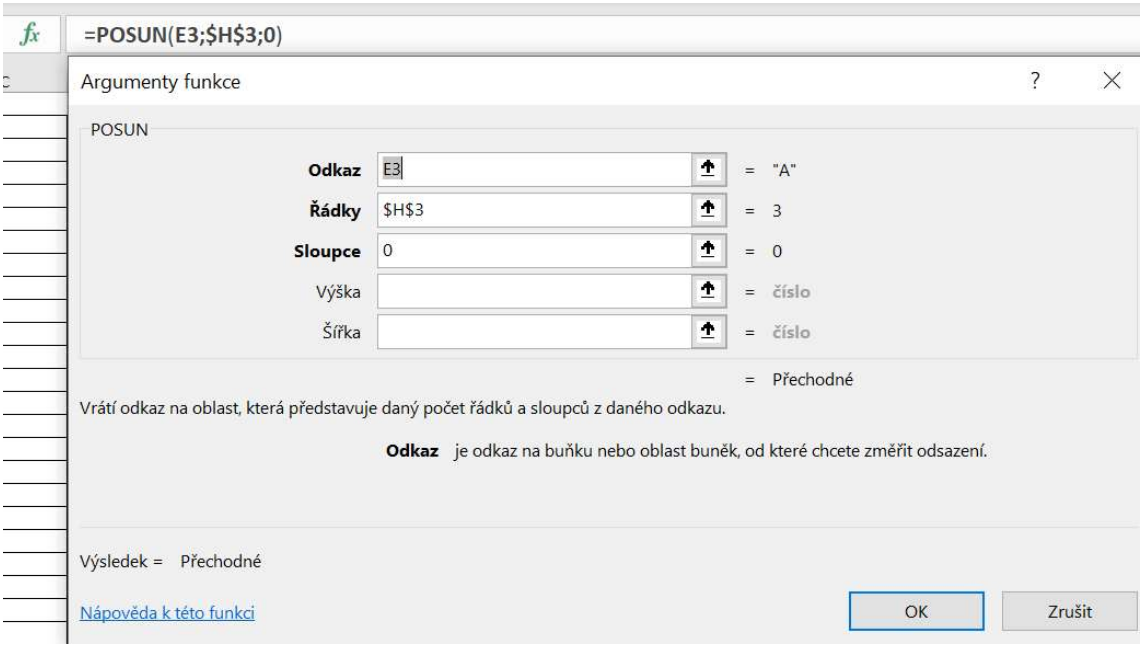
Obr. 7: Caesarova šifra krok 2 - vlastní tvorba

„Povedla se tato tabulka všem?“ Pokud má žák dotaz, tak mu na něj odpovím. „Teď přijde řada na použit první funkci POSUN, klikněte si do prvního řádku ve sloupci Kód a otevřete si vložení funkce. Tlačítko této funkce najdete v horní liště, vypadá jako fx.



Obr. 8: Caesarova šifra krok 3 - vlastní tvorba

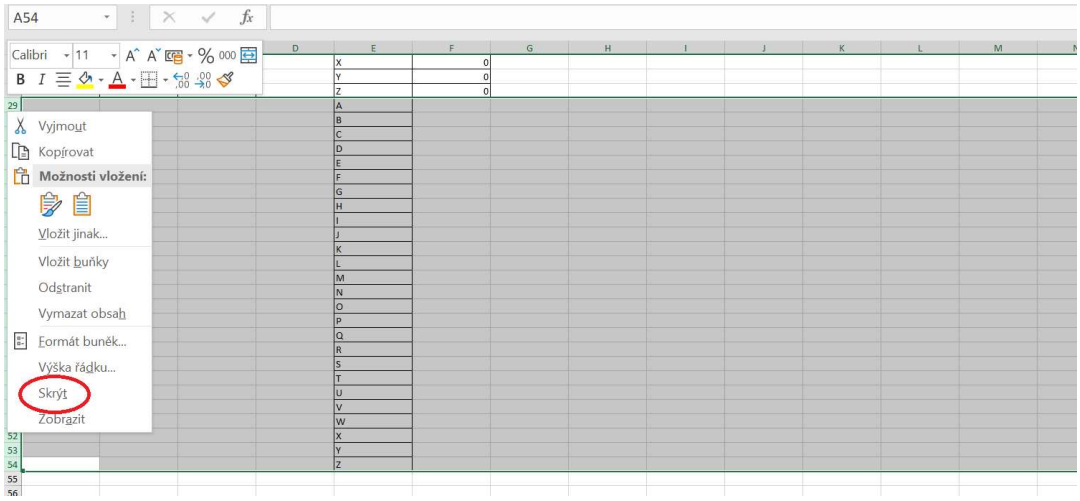
Do této buňky vložíme funkci POSUN. Při otevření této funkce se nás Excel ptá na Odkaz, Řádek a Sloupec. Funkce POSUN funguje tím způsobem, že zkopíruje danou buňku a následně ji posune. Proto do řádku Odkaz dáme buňku, ve které je písmeno A. Otázkou Řádky se nás Excel ptá, o kolik řádků má vybranou buňku posunout. Tady Vám poradím, abyste si zafixovali buňku pomocí dolaru, který napíšete Alt Gr + ů. Fixace této buňky nám pomůže s tím, že po nadefinování této buňky ji budeme moci zkopírovat pro celý řádek. Otázkou Sloupec se nás Excel ptá, o kolik sloupců chceme buňku posunout, tam dáme nulu.“



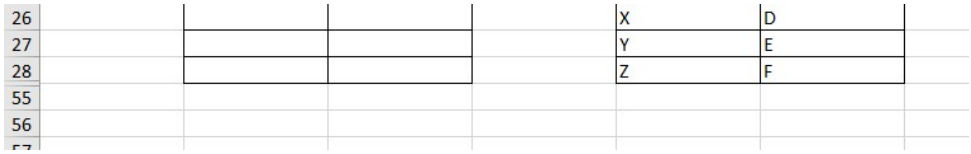
Obr. 9: Caesarova šifra krok 4 - vlastní tvorba

„Nyní, když zmáčknete tlačítko Ok, měl by Vám to fungovat. Funguje Vám to? Změní se Vám symbol, když změníte číslo v řádku Posun?“ Pokud má žák dotaz, tak mu na něj odpovím. Nyní jen nakopírujeme tuto funkci do zbylých buněk sloupce Kód. To uděláte tak, že si chytnete roh nadefinované buňky a přetáhnete ji až dolů. Za normálních okolností by nám tabulka zlobila, avšak kvůli tomu, že máme pevně zafixovaný první řádek ve sloupci Posun, tak nám tabulka funguje. Ve chvíli, kdy nebyla buňka pevně zafixovaná, tak by se funkce nadefinované buňky ptala na buňky ve sloupci Posun, které jsou na stejném řádku. Můžete s všimnout, že tabulka funguje, nicméně u posledních písmen v abecedě se nám ukazují nuly. Děje se tak z toho důvodu, že funkce Posun nemá žádnou další vyplněnou buňku, proto si zkopírujeme již vytvořenou abecedu a vložíme ji za tu stávající. Budeme mít dvě abecedy následně po sobě. Aby naše Caesarova šifra

vypadala úhledně, tuto druhou abecedu schováme. Proto si označíme řádky, na kterých je naše druhá abeceda a dáme je skrýt. Povedlo se Vám to?“ Pokud má žák dotaz, tak mu na něj odpovím.

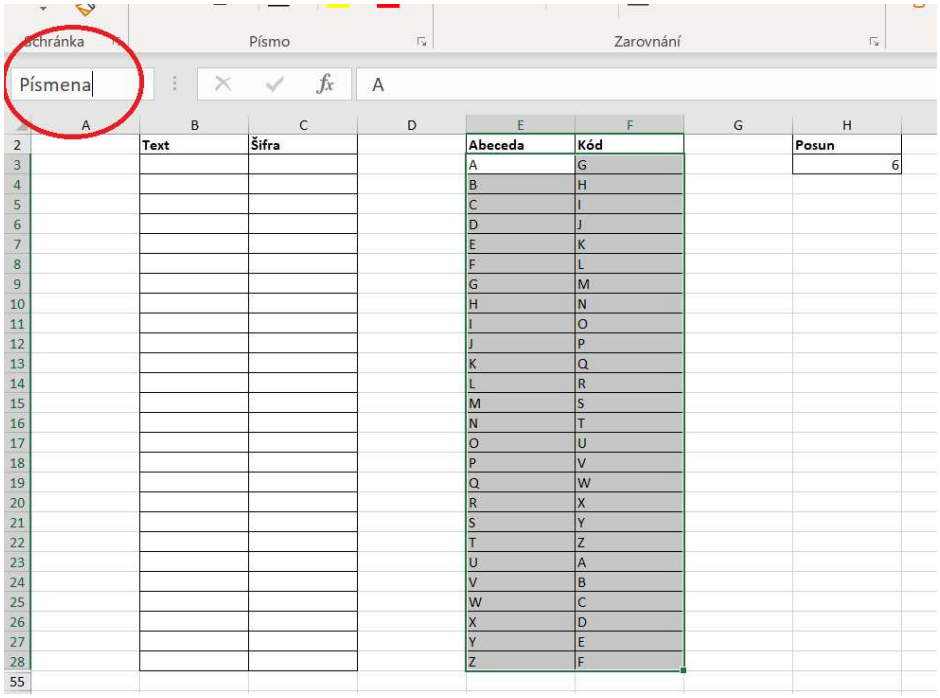


Obr. 10: Caesarova šifra krok 5 - vlastní tvorba



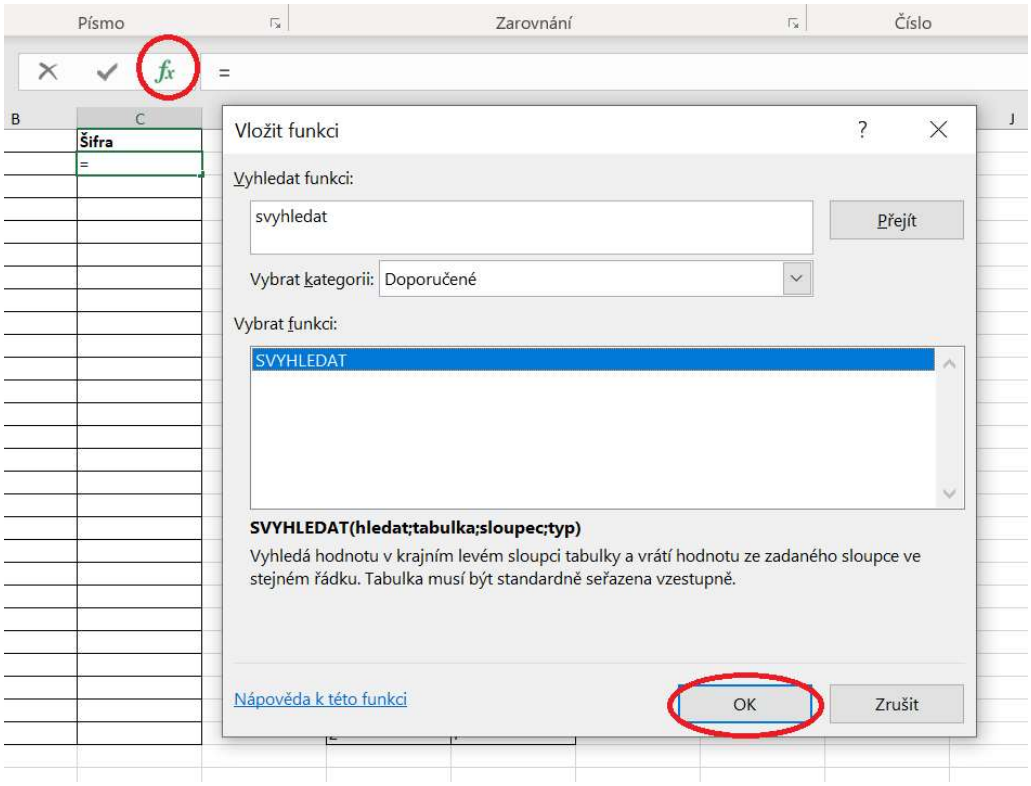
Obr. 11: Caesarova šifra krok 6 - vlastní tvorba

„Teď už máme připravenou tabulku písmen, která se nám posouvá o počet řádků, který si sami určíme. Nyní nám zbývá jen to, že se nám písmena ze sloupce Text sami změní podle námi zvoleného posunu. Výsledek se nám objeví ve sloupci Šifra. Označíme si dohromady všechny viditelné buňky ze sloupců Abeceda a Kód. Následně si tyto buňky zařadíme do oddílu, který si pojmenujeme Písmena.“



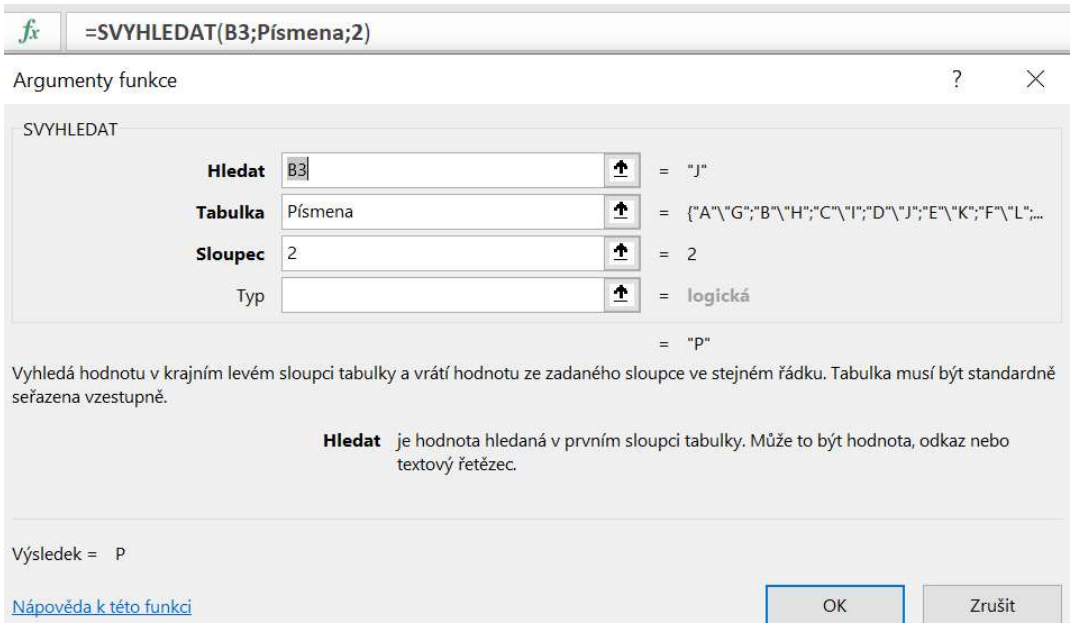
Obr. 12: Caesarova šifra krok 7 - vlastní tvorba

„Toto zařazení do oddílu nám pomůže při definování buněk sloupce Šifra. Stejně jako u funkce POSUN si i teď klikneme do první buňky sloupce Šifra. Klikneme na tlačítko funkce, které vypadá jako fx a vyhledáme si potřebnou funkci, nyní je to funkce SVYHLEDAT.“



Obr. 13: Caesarova šifra krok 8 - vlastní tvorba

„Toto potvrdíme. Funkce SVYHLEDAT po nás bude chtít nadefinovat Hledat, Tabulka, Sloupec. Otázka Hledat se nás ptá, pro který symbol hledáme odpověď, proto zde vybereme první buňku v sloupci Text. Do otázky Tabulka nemusíme označovat žádné buňky, jen napíšeme název oddílu, v našem případě Písmena. Poslední otázka Sloupec, chce vědět, který sloupec z oddílu Písmena chceme použít jako odpověď. V našem případě se ptá, ve kterém sloupci jsou zašifrované znaky, proto sem napíšeme dvojku a stiskneme ok. Povedlo se Vám to?“ Pokud má žák dotaz, tak mu na něj odpovím.



Obr. 14: Caesarova šifra krok 9 - vlastní tvorba

Nyní jen stačí námi nadefinovanou buňku zkopírovat pro zbytek řádku. Do sloupce Text teď můžete po písmenech napsat jakoukoliv zprávu a automaticky se Vám bude generovat v sloupci Šifra symbolu, podle Vámi zvoleného posunu. Povedlo se Vám to?“ Pokud má žák dotaz, tak mu na něj odpovím.

Text	Šifra
J	P
A	G
K	Q
V	B
A	G
M	S
S	Y
L	R
O	U
P	V
R	X
O	U
G	M
R	X
A	G
M	S
O	U
V	B
A	G
N	T
I	O
V	B
E	K
X	D
C	I
E	K
L	R
U	A

Abeceda	Kód
A	G
B	H
C	I
D	J
E	K
F	L
G	M
H	N
I	O
J	P
K	Q
L	R
M	S
N	T
O	U
P	V
Q	W
R	X
S	Y
T	Z
U	A
V	B
W	C
X	D
Y	E
Z	F

Posun
6

Obr. 15: Caesarova šifra krok 10 - vlastní tvorba

38–43 Shrnutí hodiny – opakování grafových algoritmů, programování Caesarovy šifry

„Dneska jsme si zopakovali látku z grafových algoritmů a žák XY nám správně vyřešil příklad na barevnost grafů. Pak jsme se bavili o Caesarově šifře, kterou jsme si v Excelu naprogramovali. Bylo dneska vše srozumitelné? Máte dotazy?“ Pokud mají žáci dotazy, tak na ně odpovím. Jelikož chci získat zpětnou vazbu na tuto vyučovací hodinu, ptám se žáků: „Co se Vám na dnešní hodině líbilo?“ Pokud žáci nereagují, doptávám se na detaily: „Nebyla pro Vás ta úloha moc těžká? Nebyl na Vás výklad moc rychlý? Orientovali jste se v programování v Excelu?“

43 – 45 Rozdání dotazníků, zhodnocení vyučovací hodiny, oznámení písemné práce

„Jsem rád, že se Vám hodina líbila. Probírali jsme základ kryptografie, která souvisí s kryptoaktivy, o kterých píšu závěrečnou práci, vyplňte mi prosím tento anonymní dotazník.“ Rozdám dotazníky. Poté, co mi je žáci odevzdají, oznámím, že si příští hodinu napíšou písemnou práci. „Děkuji Vám za vaši zpětnou vazbu, na začátku příští hodiny si pro Vás připravím test na grafové algoritmy, ale nebojte, programování, které jsme dnes dělali, tam nebude.“ Rozloučím se se třídou a odcházím.

5.2 Struktura druhé hodiny informatiky

Název: Test + Těžba kryptoaktiv

Charakteristika hodiny:

Hodina je zaměřena na zopakování získaných znalostí z předchozích hodin. V první části hodiny si žáci píšou písemnou práci. V druhá část hodiny je probráno téma těžba kryptoaktiv. Tato druhá část je formou výkladu. Žák si během lekce procvičí logické myšlení a dozví se o moderních technologiích.

Klíčová slova: grafové algoritmy, těžba kryptoaktiv

Délka hodiny: 45 minut

Kontext hodiny:

Lekce bude probíhat ve třídě druhého ročníku čtyřletého gymnázia nebo v sextě osmiletého gymnázia. Očekávaný věk žáků je 16-17 let. Tato hodina spadá v RVP G do kapitoly Informační a komunikační technologie a do podkapitoly Algoritmizace úloh. Optimální počet žáků na vyučovací hodině je dvacet čtyři. Od žáků je očekávána částečně odborná znalost z tématu předchozí vyučovací hodiny.

Touto vyučovací hodinou končíme tematický plán Algoritmizace úloh. Na tuto hodinu by měla navazovat první hodina nového tematického plánu.

Pomůcky:

- Tabule
- Projektor
- Křída nebo fix
- Připravená prezentace
- Sešit a psací potřeby
- Předpřipravená písemná práce na procvičení algoritmických úloh

Cíle hodiny:

- Žák vysvětlí užitek hashe minulého bloku a nonce při těžbě kryptoaktiv

Klíčové kompetence:

- Kompetence k učení
- Sociální a personální kompetence
- Kompetence k řešení problémů

Hodnocení:

Při hodině je hodnocena spolupráce žáků s vyučujícím a aktivní zapojení žáků v samostatné činnosti. Hodnocení je slovní. Písemná práce bude hodnocená známkou.

Uchování informací:

Žákům je umožněno zapisovat si poznámky a důležité informace do sešitů.

Časový harmonogram:

Časové rozmezí [min]	**Aktivita**
0–3	Úvod hodiny, seznámení žáků s průběhem hodiny
3–5	Motivace žáků
5–25	Písemná práce
25–35	Princip těžby kryptoaktiv
35–38	Upevnění probraného učiva – Princip těžby kryptoaktiv
38–43	Shrnutí hodiny – písemná práce, princip těžby kryptoaktiv
43–45	Rozdání dotazníků, zhodnocení vyučovací hodiny

Tab. 3: Hodina ICT 2 – vlastní tvorba

Popis aktivit:

Před začátkem hodiny

Vejdu do třídy a vítám příchozí žáky, abych je podpořil v dobrém zvyku chodit v čas. Tento čas před začátkem hodiny investuji do tvorby vztahu mezi mnou a žáky. Zajímám se o jejich názor a směji se jejich vtipům.

0–3 Úvod hodiny, seznámení žáků s průběhem hodiny

Poprosím žáky o ztišení. Přivítám žáky a seznámím je s průběhem hodiny: „Dneska si napíšeme krátkou písemnou práci a pak se podíváme, na jakém principu funguje těžba kryptoaktiv.“

3–5 Motivace žáků

Začnu se žáky diskusi: „Co si myslíte o známkování a testech ve škole?“, očekávám negativní postoj od žáků, vyslechnu žáka. „Chápu Vás, a když jsem chodil na střední, tak jsem si myslel to samé, až později mi došlo, že učitelé nemají moc způsobů zjistit, kolik toho umíme. Žádný učitel nechce dávat špatné známky, nicméně jeho prací je Vám předat znalosti a písemky jsou kontrolou, jestli Vás učí správně.“

5–25 Písemná práce

Rozdám písemné práce studentům. „Tahle písemná práce je jednoduchá, pokud něčemu nebudete rozumět, klidně se mě zeptejte.“ Nebudu žákům připomínat, jak etické je podvádět, pokud uvidím, že žáci podvádí, nebudu jim jejich práci klasifikovat a připravím pro ně novou písemnou práci, která bude náročnější. Aby poctiví žáci nebyli demotivováni, budu při klasifikaci velmi mírný.

Během psaní písemné práce dohlížím, aby v třídě byl klid a pořádek. Otevřu okno, aby se žákům lépe dýchalo. Chodím po třídě a žákům, kteří si nevědí rady, mírně napovídám.

V momentě, kdy se blíží konec časové dotace na písemnou práci, na to žáky upozorním. „Jaká byla podle Vás písemná práce? Byla moc těžká? Věděli jste si rady s jednotlivými úlohami?“ Na dotazy žáků odpovídám a doptávám se, proč mají právě tento názor. Nesoupeřím argumentačně se žáky, snažím se s nimi rozklíčovat překážky při studiu.

25–35 Princip těžby kryptoaktiv

Začátek prezentace slide 1: „Minulou hodinu jsme programovali Caesarovu šifru, pomocí které Julius Caesar šifroval své zprávy. Dnes budeme v šifrování pokračovat a podíváme se na princip těžby kryptoaktiv, při kterém se šifrování používá. Víte, co jsou to kryptoaktiva?“

Slide 2: Pokud žák ví, co jsou kryptoaktiva, nechám ho to vysvětlit a případně ho doplním. „Velmi zjednodušeně řečeno se jedná o internetové prostředky směny, který se získává tak zvanou těžbou. Která znáte kryptoaktiva?“ Pokud žáci znají některá kryptoaktiva, nebo se aktivně vyjádří k tématu, tak je pochválím. „Nejznámějším a historicky nejstarším kryptoaktivum je bitcoin, slyšeli jste už o něm?“ Pokud ano, nechám žáky, aby mi sdělili, co o něm vědí, aktivně poslouchám.

Slide 3: „Bitcoin je databáze, která jednotlivé informace ukládá do bloků. Je to jako velký deníček, ve kterém jsou jednotlivé dny jako bloky a události, co se ten den staly, jsou informace, z kterých se jednotlivé bloky skládají. Jednotlivé bloky na sebe navazují a tvoří řetězec, tomuto řetězci se říká blockchain. Za každé přidání nové informací bloku do řetězce získává přidavatel odměnu, tomuto procesu se říká těžba. Chápeme to všichni? Blockchain je databáze, která se skládá z bloků s informacemi.“ Úmyslně opakuji již řečenou informaci, abych zvýšil šanci, že žáci tento princip pochopí. „Teď se dostaneme k tomu, proč se o těžbě bavíme v souvislosti s algoritmy. Napadá někoho, co má těžba kryptoaktiv společné s algoritmy?“ Pokud žák reaguje, tak ho nechám, aby vysvětlil

problematiku těžby, a případně ho doplním. „Jak jsem již řekl, blockchain je databáze, která se skládá z bloků, které na sebe navazují. Aby na sebe mohli navazovat, potřebujeme znát informace o předchozím bloku.“

Slide 4: „Informace o minulém bloku jsou uchovávané pomocí hashe, což je jednosměrný algoritmus, který dokáže zkrátit zápis informací. Hashe na sebe v blockchainu navazují, představte si to jako posloupnost Caesarových šifer. Existovala by unikátní prvotní šifra a ostatní šifry by jen popisovaly aktualizaci této šifry, nebo by aktualizovali předchozí aktualizace. Čím delší bychom měli řetězec šifer, tím náročnější by bylo jejich prolomení, případný útočník by musel změnit všechny šifry. Vezmeme si tedy hash minulého bloku a přidáme k němu nové informace, u bitcoinu jsou to transakce, které proběhly v síti. Pokud máme tyto informace, tak potřebujeme ještě nonci. Víte, co to je? Nonce je náhodné číslo, které tipujeme. Při těžbě kryptoaktiv slouží k regulaci rychlosti těžby. Pokud zašifrujeme pomocí hashe – hash minulého bloku, transakce, které proběhly a tipnout nonci dohromady, dostaneme se k nějakému výsledku. Je do doposud pochopitelné? Máte nějaký dotaz?“ Pokud žáci mají dotaz, tak na něj odpovím. „Tento výsledek nám říká, zdali jsme tipli správnou nonci, tedy jestli můžeme přidat tento blok k ostatním blokům. Je to jednoduchý algoritmus, který říká: „Pokud výsledek hashovací funkce, do které jsi dosadil hash minulého bloku, transakce a nonci, je větší než X, nemůžeš tento blok uzavřít“, to vede k tomu, že uživatel, v tomto případě takzvaný těžař, který chce přidat nových block a získat odměnu, musí zkusit jinou nonci. Napadá někoho, pomocí čeho se také ohodnocuje cena kryptoaktiva? Jaká je forma těžařova vkladu?“ Pokud zná žák odpověď, nechám ho, aby vysvětlil formu těžařova vkladu, a případně ho doplním. „Tady tomu procesu se říká proof of work neboli důkaz prací, ve kterém těžař spotřebovává svůj výpočetní výkon počítače a energii. Napadá někoho, jak může těžař získat výhodu nad ostatními těžaři?“ Pokud zná žák odpověď, jak může těžař získat výhodu na ostatními těžaři nechám ho, aby možnost získání výhody vysvětlil spolužákům, a případně ho doplním.

Slide 5: „Těžař může získat výhodu nad ostatními v moment, kdy rychleji vypočítává hashovací algoritmus, tím pádem stihne vyzkoušet více noncí, nebo v moment, kdy má levnější energii než ostatní těžaři, protože má tím pádem na vytěženém kryptoaktivu větší zisk neboli k jeho vytěžení měl menší náklady.“

35–38 Upevnění probraného učiva – Princip těžby kryptoaktiv

„Rozumíme tedy, na jakém principu funguje těžba kryptoaktiv?“ Pokud má žák dotaz, tak mu na něj odpovím. „Jelikož jste dneska dobře pracovali, tak jsem si pro Vás připravil krátké video o dnešním tématu.“ Snažím se příležitostně používat první osobu množného čísla, ve větách, kdy se žáků ptám, z toho důvodu, aby se nad nimi nepovyšoval „já to vím a vy ne“, nicméně při pochvalách mluvím buď k jednotlivci, nebo se snažím používat druhou osobu množného čísla, aby se žáci cítili lépe, že „oni něco dokázali, oni pracovali dobře“.

Video: https://www.mall.tv/kdo-to-plati/ohrozi-tezba-bitcoinu-nasi-planetu

„Máte nějaké dotazy k těžbě kryptoaktiv?“ Pokud má žák dotaz, tak mu na něj odpovím.

38–43 Shrnutí hodiny – písemná práce, princip těžby kryptoaktiv

„Takže dneska jsme psali písemnou práci a probrali jsme princip těžbu kryptoaktiv. Je nám vše jasné, nebo máme nějaké dotazy?“ Pokud má žák dotaz, tak mu na něj odpovím. „Jak se vám dneska pracovalo? Co bych měl na hodinách zlepšit?“ Pokud žáci nereagují, tak se doptávám na detaily: „Byl ten test na Vás moc těžký? Vysvětlil jsem těžbu kryptoaktiv pochopitelně? Chtěli byste při hodině více videí?“

43–45 Rozdání dotazníků, zhodnocení vyučovací hodiny

Slide 6: „Jsem rád, že se Vám hodina líbila. Probírali jsme princip těžby kryptoaktiv, který souvisí s mojí závěrečnou prací, vyplňte mi prosím tento anonymní dotazník.“ Rozdám dotazníky. „Děkuji Vám za dnešní hodinu.“ Rozloučím se se třídou a odcházím.

5.3 Struktura třetí hodiny informatiky

Název: grafické karty, ASIC zařízení a těžba kryptoaktiv

Charakteristika hodiny:

Hodina je zaměřena na pochopení rozdílu funkce i vlastnosti grafických karet a ASIC zařízení. V první části hodiny budou mít žáci výklad s prezentací zaměřený na grafické karty a ASIC zařízení. V druhé části hodiny bude popsán princip, jakým způsobem probíhá těžba kryptoaktiv. Žák si během lekce rozšíří znalosti o hardwaru principech fungování některých databází.

Klíčová slova: hardware, grafická karta, ASIC, těžba kryptoaktiv

Délka hodiny: 45 minut

Kontext hodiny:

Lekce bude probíhat ve třídě druhého ročníku čtyřletého gymnázia nebo v sextě osmiletého gymnázia. Očekávaný věk žáků je 16-17 let. Tato hodina spadá v RVP G do kapitoly Informační a komunikační technologie a do podkapitoly Digitální technologie – hardware. Optimální počet žáků na vyučovací hodině je dvacet čtyři. Není očekávána odborná znalost tématu ze strany žáků. Je však předpokládáno, že žák se již s termínem grafická karta setkal.

Tato vyučovací hodina ukončuje tematický plán (Hardware). Na tuto hodinu by měla navazovat opakovací hodina, která by shrnula dané téma. V opakovací hodině by si měli žáci zopakovat získané znalosti o hardwaru – základní deska, procesor, RAM paměť, pevný disk, grafická karta.

Pomůcky:

- Tabule
- Projektor
- Křída nebo fix
- Připravená prezentace
- Sešit a psací potřeby

Cíle hodiny:

- Žák na příkladech popíše rozdíl mezi těžbou na grafické kartě a ASIC zařízením

Klíčové kompetence:

- Kompetence k učení
- Kompetence k řešení problémů
- Sociální a personální kompetence

Hodnocení:

Při hodině je hodnocena spolupráce žáků mezi sebou i s vyučujícím. Hodnocení je slovní.

Uchování informací:

Žákům je umožněno zapisovat si poznámky a důležité informace do sešitů.

Časový harmonogram:

Časové rozmezí [min]	**Aktivita**
0–3	Úvod hodiny, seznámení žáků s průběhem hodiny
3–5	Motivace žáků ke znalosti hardwaru
5–15	Opakování předchozího učiva ve skupinkách
15–20	Grafické karty
20–25	ASIC zařízení
25–30	Teorie her těžby kryptoaktiv
30–38	Fixace probraného učiva – grafické karty, ASIC zařízení, teorie her těžby kryptoaktiv
38–43	Shrnutí hodiny – opakování ve dvojicích, grafické karty, ASIC zařízení, teorie her těžby kryptoaktiv
43–45	Rozdání dotazníků, zhodnocení vyučovací hodiny

Tab. 4: Hodina ICT 3 – vlastní tvorba

Popis aktivit:

Před začátkem hodiny

Vejdu do třídy a vítám příchozí žáky, abych je podpořil v dobrém zvyku chodit v čas. Tento čas před začátkem hodiny investuji do tvorby vztahu mezi mnou a žáky. Zajímám se o jejich názor a směji se jejich vtipům.

0–3 Úvod hodiny, seznámení žáků s průběhem hodiny

Poprosím žáky o ztišení. Přivítám žáky a seznámím je s průběhem hodiny: „Dneska si zopakujeme látku z minulé hodiny, probereme grafickou kartu a ASIC zařízení. Na konci, pokud nám zbude čas, probereme těžbu kryptoaktiv.“ Používám výraz „pokud nám zbude čas“, abych naznačil, že nám hodina rychle uteče.

3–5 Motivace žáků ke znalosti hardwaru

Začnu se žáky diskusi: „Zkoušeli jste si někdy sestavit vlastní počítač?“ Pokud se žák přihlásí, že zkoušel, povídám si s ním o komponentech. „Co byste potřebovali znát, abyste si mohli sestavit vlastní počítač? Jak poznáte, že jste vybrali správné součástky?“ Nenásilnými otázkami se snažím dovést žáky k myšlence, proč je znalost hardwarových komponent v běžném životě užitečná. Celou motivační část zakončuji otázkou: „Jaký by měl být Váš počítač? K čemu byste ho používali?“ Podobnými otázkami žákům ukazuji, že pokud se budou orientovat v hardwarových komponentech, mohou si eventuelně sestavit počítač přesně podle jejich představ.

5–15 Opakování předchozího učiva ve skupinkách

„Nyní prosím utvořte před tabulí řadu, podle abecedy.“ Následně žáky rozdělím do dvojic. Tímto způsobem utvořím dvojce, které nebudou sestaveny na základě sympatií žáků mezi sebou, snažím se tak zlepšit jejich sociální dovednosti, žák se může blíže seznámit se svými spolužáky. Navíc se při této aktivitě aspoň trochu žák protáhne. „Vaším úkolem ve dvojici bude to, že si spolu zopakujete klíčové znalosti z minulé hodiny, pokud si nějakou informací nebudete jistí, můžete se zeptat mě, nebo jiné skupinky.“ Při této aktivitě chodím mezi dvojicemi a hlídám pořádek ve třídě. Moje interakce s jednotlivými skupinkami je založena na položení otázky a následné pochvale: „Jak se Vám líbila minulá hodina? Co si z ní pamatujete? Dobře jste si to zapamatovali.“ Případně skupinkám radím a podněcuji konverzaci. Během této aktivity si připravuji prezentaci. „Líbí se mi, jak pracujete ve dvojicích, na čem se Vaše dvojce shodla jako na nejpodstatnější informaci z minulé hodiny.“ Tímto způsobem přiměju skupinku krátce interagovat se zbytkem třídy. „Dobře, tak se prosím vraťte na místa a začneme s těmi grafickými kartami.“

15–20 Grafické karty

Začátek prezentace: „Dnes se podíváme na další část hardwaru a tou jsou grafické karty. Víte, k čemu slouží grafická karta u vás v počítači? Můžete mi dát nějaký příklad?“ Slide 2: Pokud zná žák odpověď, nechám ho, aby vysvětlil, co je grafická karta a případně ho doplním. „Grafická karta slouží k vykreslení obrazu na monitoru a skládá se z integrovaného procesoru, operační paměti, napájecí kaskády, chlazení, výstupů, komunikační sběrnice a přídavné napájení.“ Slide 3: „Procesor grafických karet se označuje GPU z anglického graphics processing unit a má na starost grafické výpočty,

které slouží k vykreslení obrazu na monitoru. Další komponentou v grafických kartách je operační paměť, do které se ukládají informace potřebné pro fungování procesoru. Napájecí kaskáda slouží k napájení grafické karty, chlazení zajišťuje, že se grafická karta nepřehřívá, přes výstupy propojujeme grafickou kartu s monitorem, komunikační sběrnice má na starost komunikaci mezi grafickým procesorem a procesorem na základní desce. Rozumíte všemu, nebo mám něco zopakovat?“ Pokud má žák dotaz, tak mu na něj odpovím. „Jaké jsou pro Vás nejdůležitější parametry při výběru grafické karty?“ Na odpovědi žáků pozitivně reaguji a navazuji na ně otázkou: „Z jakého důvodu sis vybral tento parametr?“ Pokud žáci nereagují, začnu se ptát jednotlivých žáků. „Při výběru grafické karty je dobré se rozhodovat podle grafického jádra, operační paměti, typu sběrnice. V grafickém jádru je uložený procesor. Toto jádro má určitou plochu, čím větší plocha, tím více procesorů, čím více procesorů, tím větší výkon. Pro grafické jádro také platí, že čím vyšší frekvence, tím efektivnější jádro. Při výběru grafických karet také nezapomeňte na typ operační paměti. V dnešní době je standardem DDR5, DDR5X, DDR6 a HBM. Karty typu DDR3 a DDR4 jsou již zastaralé. Jak jde technologie dopředu, tak i náročnost a propustnost sběrnic se změnila, dnes je standardem propustnost 16 až 32 GB/s. Pochopili jste vše, jsou grafické karty srozumitelné?“ Pokud má žák dotaz, tak mu na něj odpovím. „Teď už víme, že grafické karty mají velký výpočetní výkon, na co jiného byste je použili kromě vykreslování obrazu?“ Pokud zná žák odpověď, nechám ho, aby vysvětlil další využití grafických karet, a případně ho doplním. „Grafické karty se používají k náročným matematickým úlohám. Těžaři kryptoaktiv používají jejich výpočetní výkon k těžbě kryptoaktiv.“

20–25 ASIC zařízení

Slide 4: „Víte, co je to ASIC zařízení?“ Pokud zná žák odpověď, nechám ho, aby vysvětlil, co je ASIC zařízení a případně ho doplním. „ASIC je zkratka z anglického „Application Specific Integrated Circuit“. Jak byste to přeložili a zvládnete tento pojem vysvětlit vlastními slovy?“ Pokud zná žák odpověď, nechám ho, aby vysvětlil ASIC zařízení vlastními slovy, a případně ho doplním. „ASIC lze přeložit jako zařízení s integrovaným obvodem pro konkrétní aplikaci, nicméně co to znamená v praxi? Jedná se o zařízení, které je sestrojeno k jednomu konkrétnímu úkonu, který zvládá dokonale, nicméně nevýhodou tohoto zařízení je, že na ostatní funkce se zařízení nehodí. Tyto zařízení se používají například pro těžbu kryptoaktiv. ASIC zařízení funguje podobně jako sekačka na trávu. Trávu s ní posečete, ale chléb si s ní krájet nebudete. Za jakým

účelem by bylo dobré mít doma ASIC zařízení?“ Pokládám řečnické otázky, abych si na ně mohl vzápětí odpovědět. „ASIC zařízení jsou tak specifická svým využitím, takže by se Vám doma nevyplatila používat, je to jako byste měli počítač, na kterém by dokonale šlapal Word a Excel, ale žádné další aplikace. Jak jsem již zmínil, ASIC zařízení je vysoce efektivní, třeba při těžbě kryptoaktiv, v tomto videu si můžeme představit, že dospělí muž je ASIC zařízení a jeho soupeř je procesor.“

Slide 5: Pustím vtipné video – https://www.youtube.com/watch?v=3-7WL3KPmhI, které budu mít dopředu uloženo v počítači, abych se vyhnul problémům s internetem, a tím plynoucí ztrátě pozornosti od studentů. „Pochopili jste vše, bylo to pro Vás srozumitelné?“ Pokud má žák dotaz, tak mu na něj odpovím.

25–30 Teorie her těžby kryptoaktiv

Slide 6: „Když jsme zmínili tu těžbu, víte, jak probíhá těžba kryptoaktiv, třeba bitcoinu? Slyšeli jste o tom něco?“ Začíná krátká diskuze, při které zjistím aktuální stav znalostí studentů daného tématu. Následně ukončím diskuzi a slovně hodnotím aktivitu žáků. „Abychom těžbě kryptoaktiv dali hlavu a patu. Těžba kryptoaktiv do svého procesu zahrnuje mnoho různých subjektů, hlavními dvěmi je těžař a uživatel. Těžaři se mezi sebou předhánějí, kdo rychleji vytěží kryptoaktivum. Samotná těžba není zjednodušeně řečeno nic jiného než tipování náhodného čísla, takzvané nonce. Toto náhodné číslo, nonce, může být kdekoliv mezi 0 a 4 294 967 296. Proces těžby většiny kryptaktiv se dá přirovnat ke hře „Člověče, nezlob se“. Slide 7: „Tato hra je transparentní v tom, že všichni hráči vidí, jaké číslo padlo na kostce a o kolik polí se má panáček posunout. Všichni hráči vidí, že hráč při posouvání panáčkem nepodvádí, a kdyby podváděl, mohou ho potrestat. Představme si situaci, že u stolu sedí 4 hráči, kteří zaplatili startovné, ale jen první hráč, který dojde do cíle se všemi figurkami, vyhrává odměnu. Tímto způsobem se dal zjednodušeně vysvětlit proces těžby kryptoaktiv. V této hře, stejně jak při těžbě mají všichni hráči stejná pravidla. Získání nonce je v rukou náhody, jako při hodu kostkou. Hráči vidí hozená čísla na kostce a mohou kontrolovat, o kolik políček se posouvají ostatní hráči. Těžaři si zase mohou ověřit, zdali je získaná nonce správná. Startovné ostatních hráčů je energie, kterou těžař spotřebuje pro získání hashe, avšak jen první těžař získá odměnu v podobě kryptoaktiva, jehož hodnota zpravidla odpovídá hodnotě propálené energie, stejně jako první hráč v domečku získává odměnu. Pochopili jste vše, bylo to pro Vás srozumitelné?“ Pokud má žák dotaz, tak mu na něj odpovím. „Těžaři někdy těží na vícero zařízení najednou, takzvané serverové farmy. To si můžeme

představit, jako kdyby jeden hráč měl více hodů kostkou a mohl by si vybrat, svůj nejlepší hod. Serverové farmy jsou velké haly naplněné ASIC zařízeními. Další variantou těžby jsou takzvané pooly, do češtiny to jako bazény nikdo nepřekládá. Tento způsob těžby si můžeme představit tak, že by se více hráčů domluvilo, že pokud vyhrají, tak si mezi sebou rozdělí výhru."

30–38 Fixace probraného učiva – grafické karty, ASIC zařízení, teorie her těžby kryptoaktiv

„Tohle bylo pro dnešní výklad vše, teď Vás poprosím, abyste udělali stejné dvojce jako na začátku hodiny a řekli si, co nového jste se naučili?" Při této aktivitě chodím mezi dvojicemi a hlídám pořádek ve třídě. Pokud jsem si všiml, že nějaký žák nedával při hodině pozor, dojdu se ho během této aktivity zeptat, co si zapamatoval.

38–43 *Shrnutí hodiny – opakování ve dvojicích, grafické karty, ASIC zařízení, teorie her těžby kryptoaktiv*

„Bylo dnes vše pochopitelné?" Pokud má žák dotaz, tak mu na něj odpovím. Začnu se ptát třídy na již zmíněné informace. Slide 3: „Co jsme si dneska řekli o grafických kartách? K čemu slouží grafické karty? Jaké má grafická karta komponenty? Pamatujete si, k čemu jednotlivé komponenty slouží? Podle čeho si budete vybírat grafickou kartu?" Pokud žák pohotově reaguje, tak ho pochválím a pokračuji v opakování dnešní hodiny. Slide 5: „Co si pamatujete o ASIC zařízení? Vysvětlil jsem správně princip jeho fungování?" Slide 7: Co si myslíte o těžbě kryptoaktiv?"

43 – 45 Rozdání dotazníků, zhodnocení vyučovací hodiny

Slide 8: „Dnes se mi s Vámi dobře pracovalo. Probírali jsme grafické karty, ASIC zařízení a princip těžby kryptoaktiv, tyto témata souvisí s mojí závěrečnou prací, vyplňte mi prosím tento anonymní dotazník." Rozdám dotazníky. „Děkuji Vám za dnešní hodinu." Rozloučím se se třídou a odcházím.

6 Návrhy modelových hodin ZSV

6.1 Struktura první hodiny ZSV

Název: Úvod do tématu měn

Charakteristika hodiny:

Hodina je zaměřena na pochopení pojmu měna. V první části hodiny je pro žáky připravena aktivita do skupin po 2-3 členech. V druhé části hodiny jsou žáci seznámeni s pojmy měna, digitální měna, virtuální měna a krypto měna (krypto aktivum). Celková lekce uvádí žáky do problematiky forem peněz.

Klíčová slova:

peníze, měna, digitální měna, virtuální měna, kryptoměna (kryptoaktivum)

Délka hodiny: 45 minut

Kontext hodiny:

Lekce bude probíhat ve třídě prvního ročníku čtyřletého gymnázia nebo v kvartě osmiletého gymnázia. Očekávaný věk žáků je 14-16 let. Tato hodina spadá v RVP G do kapitoly Člověk a svět práce, podkapitola Finance. Optimální počet žáků je dvacet čtyři. Není očekávána odborná znalost tématu ze strany žáků. Je však předpokládána znalost vlastností peněz.

Tato vyučovací hodina navazuje na vyučovací hodinu úvod do tématu peněz. Na tuto hodinu by měla navazovat výuka týkající se kryptoaktiv.

Pomůcky:

- Tabule
- Projektor
- Křída nebo fix
- Připravená prezentace
- Sešit a psací potřeby

Cíle hodiny:

- Žák vyjmenuje rozdíly mezi digitální a virtuální měnou

- Žák formuluje aspoň tři formy měn

Klíčové kompetence:

- Kompetence k učení
- Komunikativní kompetence
- Sociální a personální kompetence
- Kompetence k řešení problémů

Hodnocení:

Při hodině je hodnocena skupinová práce mezi studenty, spolupráce žáků s vyučujícím a aktivita žáků. Hodnocení je slovní.

Uchování informací:

Žákům je umožněno zapisovat si poznámky a důležité informace do sešitů.

Časový harmonogram hodiny:

Časové rozmezí [min]	**Aktivita**
0–3	Úvod hodiny, seznámení žáků s průběhem hodiny
3–5	Motivace žáků k finanční gramotnosti
5–13	Opakování ve dvojicích
13–17	Fiat měna
17–22	Digitální měna
22–28	Virtuální měna
28–38	Kryptoměna (kryptoaktivum)
38–43	Shrnutí hodiny – Fiat měna, digitální měna, virtuální měna, kryptoměna (kryptoaktivum)
43–45	Rozdání dotazníků, zhodnocení vyučovací hodiny

Tab. 5: Hodina ZSV 1 – vlastní tvorba

Popis aktivit:

Před začátkem hodiny

Vejdu do třídy a vítám příchozí žáky, abych je podpořil v dobrém zvyku chodit v čas. Tento čas před začátkem hodiny investuji do tvorby vztahu mezi mnou a žáky. Zajímám se o jejich názor a směji se jejich vtipům.

0–3 Úvod hodiny, seznámení žáků s průběhem hodiny

Poprosím žáky o ztišení. Přivítám žáky a seznámím je s průběhem hodiny: „Dneska budeme pokračovat v tématu finance, tím způsobem, že si řekneme, co je to měna, ukážeme si různé druhy měn.

3–5 Motivace žáků

„Minulou hodinu jsme se bavili o penězích, tak jsem si doma vyhledával statistiky, jak lidé umí hospodařit, a zjistil jsem, že více než 10 % Čechů má půjčku. Čím si myslíte, že je to zapříčiněno?“ Zahajuji diskusi se žáky, během které by měli žáci přijít sami k závěru, že je správné si dělat finanční rezervu. „Řekli jste mnoho dobrých nápadů, kvůli kterým jsou lidé zadlužení. Jsem rád, že jsme se všichni shodli, že je to tím, že si lidé netvoří finanční rezervu.“

5–13 Opakování ve dvojicích

„Než začneme probírat nové téma, zopakujeme si vlastnosti peněz, postavte se, prosím, a udělejte dvojice tak, abyste byli ve dvojce s někým, kdo nesedí ve stejné řadě jako vy. Práce ve dvojicích bude probíhat tím způsobem, že si jeden z dvojce řekne vlastnost peněz a druhý mu ji vysvětlí. Máme 3 základní vlastnosti peněz: zaměnitelnost, skladovatelnost a dělitelnost.“ Tato aktivita má vést k propojování vztahů ve třídě. Během této aktivity procházím mezi jednotlivými skupinkami a dohlížím na klid ve třídě. Také si připravím prezentaci. „Super, pěkně pracujete, teď se, prosím, posaďte zpět na svá místa.“ Poté vyvolám tři žáky, aby před třídou zopakovali vlastnosti peněz.

13–17 Fiat měna

Začátek prezentace: „Abychom smysluplně navázali na předchozí hodinu, tak si dneska popovídáme o měnách.“ Slide 2: „Tou neznámější měnou je fiat měna. Jedná se o fyzické peníze, jak je známe. Fiat měna má centrální autoritu, která za ni zodpovídá, nejčastěji se jedná o národní banku. Fiat měnou jsou koruny, eura, dolary. Máte k fiat měně nějaký dotazy?“ Pokud má žák dotaz, tak mu na něj odpovím.

17–22 Digitální měna

Slide 3: „Co Vás napadne pod pojmem digitální měna a jak se podle Vás liší od fiat měny?“ Pokud zná žák odpověď, nechám ho, aby vysvětlil, co je digitální měna a popíše rozdíl mezi fiat měnou a digitální měnou, případně žáka doplním. „Digitální měna je digitalizovaná forma peněz. Setkáváme se s ní, když používáme internetové bankovnictví. I tato měna má centrální autoritu. Rozdíl mezi fiat měnou a digitální měnou je především ten, že digitální měna je nehmatatelná. Máte k digitální měně nějaký dotazy?“ Pokud má žák dotaz, tak mu na něj odpovím.

22–28 Virtuální měna

Slide 4*:* „Co Vás napadne pod pojmem virtuální měna a jak se podle Vás liší od fiat měny a digitální měny?“ Pokud zná žák odpověď, nechám ho, aby vysvětlil, co je virtuální měna a její rozdíl mezi fiat měnou a digitální měnou, případně žáka doplním. „Virtuální měna, se kterou se setkávají především hráči počítačových her. Virtuální měna se nejčastěji získává směnou za peníze, nebo za splnění nějakého specifického úkolu. V dnešní době můžeme u některých společností vyměnit virtuální měnu za statek, který má reálnou finanční hodnotu, například za Nintendo body si můžete nakoupit software od společnosti Nintendo nebo ve hře World of Warcraft si můžete za získané goldy koupit herní čas. Napadají Vás další příklady virtuálních měn?“ Dávám prostor žákům, pokud je žák aktivní, slovně po pochválím. „Máte k virtuální měně nějaké dotazy?“ Pokud má žák dotaz, tak mu na něj odpovím.

28–38 Kryptoměna (kryptoaktivum)

Slide 5: „Poslední typ měny, kterou si zmíníme je kryptoměna. Zařadil jsem kryptoměny do této hodiny, i když se prakticky nejedná o měnu, protože neexistuje žádný stát, nebo společnost, která by kryptoměny zaštitovala. Proto budu používat přesnější termín kryptoaktiva. Krypto od slova kryptografie neboli šifrování a aktivum, jako označení něčeho, co má svoji hodnotu. Setkali jste se již s pojmem kryptoměna, nebo kryptoaktiva? Znáte nějaká kryptoaktiva“ Pokud se žák s tímto pojmem již setkal, nechám žáka, aby řekl, jaké znalosti o kryptaktivech má, případně ho doplním. „Víte proč se kryptoaktiva spojují s penězi?“ Pokud má žák nějaké nápady, pochválím ho a ocením jeho aktivitu. „Kryptoaktiva jsou spojována s penězi, protože se mnozí lidé používají stejně, jako digitální měnu. Každé kryptoaktivum má jiné vlastnosti, tou základní je decentralizovanost, tím se myslí to, že nemají nad sebou žádnou autoritu a uživatelé se

o svoji síť starají sami. Funguje to tak, že všichni uživatelé jsou pseudoanonymní, je to jako když si v online počítačové hře vytvoříte postavu a komunikujete s ostatními hráči, nikdo neví, kdo tuto postavu ovládá. Ve světě kryptoaktiv má každý uživatel svoji peněženku a všichni ostatní uživatelé vědí, kolik daného aktiva má na této peněžence. Pokud si uživatel A řekne, že pošle část svých aktiv uživateli B, všichni uživatelé o tom ví, nicméně nikdo nezná identitu těchto uživatelů. Někteří lidé si vytvoří více peněženek z důvodu větší bezpečnosti. Napadá Vás, v čem je další výhoda kryptoaktiv?“ Pokud má žák nějaké nápady, pochválím ho a ocením jeho aktivitu. „Díky tomu, že je vše decentralizované a pseudoanonymní tak transakce v sítích kryptoaktiv jsou zpravidla velmi rychlé. Abych tu rychlost uvedl na správnou míru, v bitcoinové síti trvá transakce cirka 10 minut, takže pokud byste chtěli platit bitcoinem v obchodě, tak byste se celkem načekali, avšak s porovnáním, jak dlouho trvají například odesílání transakcí o víkendu, je toto rychlovka. Bitcoin neřeší v jaký čas a do jaké země aktiva posíláte. Vidíte v kryptaktivech potenciál do budoucna?“ Pokud má žák nějaké nápady, pochválím ho a ocením jeho aktivitu. „Mnoho lidí vidí v kryptaktivech budoucí prostředek směny. Jejich argumenty mi připadají logické, lidem vadí to, že v centralizovaném systému ztrácí svobodu zacházet libovolně se svými penězi, na druhou stanu si tito lidé neuvědomují, že díky centrálnímu systému mají nad sebou autoritu, za kterou mohou jít, když se jim něco pokazí. Co si o tom myslíte vy?“ Pokud má žák nějaké nápady, pochválím ho a ocením jeho aktivitu. „Máte ke kryptoaktivům nějaký dotazy?“ Pokud má žák dotaz, tak mu na něj odpovím.

38–43 Shrnutí hodiny – historie a vlastnosti peněz

„Na začátku dnešní hodiny jsme si zopakovali základní vlastnosti peněz: zaměnitelnost, skladovatelnost a dělitelnost. Následně jsme spolu probrali vlastnosti jednotlivých měn, řekli jsme si, co je to fiat měna – papírové peníze, digitální měna – digitální peníze, třeba v internetovém bankovnictví, virtuální měna – měna, se kterou se setkáváme například v počítačových hrách a kryptoaktiva – decentralizovaná, pseudoanonymní alternativa fiat měny. Máte k měnám nějaké dotazy?“ Pokud má žák dotaz, tak mu na něj odpovím.

43–45 Rozdání dotazníků, zhodnocení vyučovací hodiny

„Jak se Vám dnešní hodina líbila a co byste na ní zlepšili? Jak na Vás působilo téma měn? Chcete více prostoru v hodinách, pro vyjádření názorů? Co byste chtěli dál probírat, co Vás zajímá?“ Vyslechnu si názor žáků a objektivně zhodnotím dnešní hodinu, avšak

nekritizuji. „Poprosím Vás, abyste mi na závěr vyplnili krátký anonymní dotazník.“ Rozdám dotazníky.

Slide 6: „Děkuji Vám za dnešní hodinu.“ Rozloučím se se třídou a odcházím.

6.2 Struktura druhé hodiny ZSV

Název: Kryptoaktiva a jejich hodnota

Charakteristika hodiny:

Hodina je zaměřena na kryptoaktiva a jejich hodnotu. V první části hodiny si žáci zopakují základní vlastnosti a funkce peněz. V druhé části hodiny je žákům vysvětleno, čím se určuje cena produktu. Ve třetí části hodiny se probírá hodnota kryptoaktiva jako aktiva. Ve čtvrté části se žáci dozvědí o využití kryptoaktiv jako platebního nástroje. Na závěr hodiny jsou informace uceleny a sjednoceny. Vyučovací hodina učí žáka pracovat s kryptoaktivy.

Klíčová slova: kryptoaktiva, aktiva, cena, prostředek směny.

Délka hodiny: 45 minut

Kontext hodiny:

Lekce bude probíhat ve třídě prvního ročníku čtyřletého gymnázia nebo v kvartě osmiletého gymnázia. Očekávaný věk žáků je 14-16 let. Tato hodina spadá v RVP G do kapitoly Člověk a svět práce, podkapitola Finance. Optimální počet žáků je dvacet čtyři. Je očekávána částečně odborná znalost tématu kryptoaktiva ze strany žáka. Tento předpoklad vyplívá z předchozích dvou hodin: Úvod do tématu peněz, Úvod do tématu měn.

Pomůcky:

- Tabule
- Křída nebo fix
- Projektor
- Připravená prezentace
- Sešit a psací potřeby
- Předpřipravenou studijní tabulku s rozdíly mezi penězi a kryptoaktivy

Cíle hodiny:

- Žák formuluje, na jakém základě se určuje cena produktů

Klíčové kompetence:

- Kompetence k učení
- Komunikativní kompetence
- Sociální a personální kompetence
- Kompetence k řešení problémů

Hodnocení:

Při hodině je hodnocena skupinová práce žáků, spolupráce žáků s vyučujícím a aktivita žáků během vyučovací hodiny. Hodnocení je slovní.

Uchování informací:

Žáci na konci hodny obdrží předpřipravenou studijní tabulku s rozdíly mezi penězi a kryptoaktivy. Žákům je umožněno zapisovat si poznámky a důležité informace do sešitů.

Časový harmonogram hodiny:

Časové rozmezí [min]	**Aktivita**
0–3	Úvod hodiny, seznámení žáků s průběhem hodiny
3–5	Motivace žáků ke studiu
5–15	Zopakování základních vlastností peněz a kryptoaktiv
15–23	Určování ceny
23-30	Kryptoaktivum jako aktivum
30–38	Využití kryptoaktiv jako platebního nástroje
38–43	Shrnutí hodiny a rozdání studijní tabulky
43–45	Rozdání dotazníků a předpřipravených listů, zhodnocení vyučovací hodiny

Tab. 6: Hodina ZSV 2 – vlastní tvorba

Popis aktivit:

Před začátkem hodiny

Vejdu do třídy a vítám příchozí žáky, abych je podpořil v dobrém zvyku chodit v čas. Tento čas před začátkem hodiny investuji do tvorby vztahu mezi mnou a žáky. Zajímám se o jejich názor a směji se jejich vtipům.

0–3 Úvod hodiny, seznámení žáků s průběhem hodiny

Poprosím žáky o ztišení. Přivítám žáky a seznámím je s průběhem hodiny: „Dneska probereme základní faktory, které určují cenu zboží, definujeme si to, co je to aktivum a ukážeme si využití kryptoaktiv jako prostředku směny."

3–5 Motivace žáků ke studiu

Začínám diskuzi: „Připadá Vám tato hodina užitečná? Vidíte v ní smysl? Myslíte si, že tyto znalosti využijete v běžném životě, nebo v práci?", čekám na reakci žáka, s jeho názorem vždy souhlasím a neoponuji mu. „Jak vnímáte školu? Jsou zde nějaké předměty, které Vám připadají zbytečné?" Během této diskuze, se snažím, aby žák pochopil, že co pro mu připadá zbytečné, není zbytečné pro jeho spolužáky. Tento myšlenkový pochod vede žáka k toleranci.

5–15 Zopakování základních vlastností peněz a kryptoaktiv

„V minulých hodinách jsme probírali vlastnosti a funkce peněz, co si z tohoto tématu pamatujete?" Dávám žáku prostor, aby se vyjádřil, a případně ho doplním. Pokud žák nereaguje, ptám se na konkrétnější otázky: Proč vznikli peníze? K čemu slouží peníze? Jak používáte peníze? Poté, co si zopakujeme základní vlastnosti peněz, zopakuji si se žáky ještě základní vlastnosti kryptoaktiv. Ptám se žáků: Co jsou to kryptoaktiva? Znáte příklad nějakého kryptoaktiva? Kde se s ním můžeme setkat? K čemu se používá?

15–23 Určování ceny

Slide 1. „Přemýšleli jste na tím, co určuje cenu zboží? Ano, určují ji firmy, tím základním faktorem je nabídka a poptávka. Čím je daného zboží na trhu méně, tím více stojí."

Slide 2. „Toto je smyšlený příběh, na kterém si můžeme demonstrovat, jak to nabídka a poptávka funguje. Žil jeden bohatý pán, který měl tu nejvzácnější známku na světě, byla unikátní. Jednoho dne mu na verandě zazvonil malý chlapec, že na půdě u dědečka našel tu stejnou známku, kterou vlastnil bohatý pán. Bohatý pán mu za ni nabídl velké množství

peněz a chlapec na to kývnul. Víte, co udělal bohatý muž s touto známkou? Spálil ji, protože kdyby existovali dvě stejné, ta jeho by již nebyla unikátní a ztratila by svoji cenu. Na obrázku můžete vidět aktuálně nejvzácnější známku světa z roku 1847, která se jmenuje Modrá perla z Mauricia. Stojí 64 miliónů korun. Napadá Vás nějaký vliv nabídky a poptávky, se kterým jste se setkali?“ Dávám prostor žákům, pokud je žák aktivní, slovně ho pochválím. „Například v roce 2020 během koronavirové pandemii klesla cena pohonných paliv kvůli tomu, že méně lidí cestovalo a paliv byl nadbytek. Cenu neovlivňuje pouze množství daného zboží na trhu, ale i jeho užitečnost. Čím je zboží užitečnější, tím větší bude mít cenu. Například, kdyby vědci objevili, že čokoláda v sobě obsahuje vitamíny. V ten moment by pro lidi měla čokoláda větší užitek, který by se projevil na její ceně. Množství a užitek zboží jsou základní dva faktory určující cenu. Firmy, které dané zboží distribuují, musí do svých nákladů započítat marketing, export zboží, zaměstnance a marže. Je logické, že firmy nebudou chtít prodávat zboží, které svoji cenou nepokryje svoji výrobu. Firmy mohou také hýbat s cenou svých produktů, aby si ustálili místo na trhu. Společnosti s menšími náklady mohou snížit cenu produktů, za účelem získání výhody před konkurencí, která může na základě vyšší ceny přijít o své zákazníky. Pokud konkurence také sníží cenu, tak přichází o zisk, který mohla investovat do inovací. Avšak o tom si povíme příště, pro dnešek nám bude stačit pochopení výrobních nákladů, nabídky a poptávky. Máme nějaký dotaz k nabídce, poptávce, nebo výrobním nákladům?“ Pokud má žák dotaz, tak mu na něj odpovím.

23–30 Kryptoaktivum jako aktivum

Slide 3. „Setkali jste se někdy s pojmem aktivum?“ Dávám prostor žákům, pokud se žák s pojmem aktivum již setkal, nechám ho, aby pojem aktivum vysvětlil svým spolužákům, a slovně po pochválím. „Aktivum obecně chápeme jako něco, co přináší vlastníkovi nějaký výnos, nebo se očekává, že ho přinese v budoucnu. Aktiva můžeme rozdělit podle několika parametrů, těmi základními dvěmi jsou aktiva reálná a finanční. Mezi reálná aktiva řadíme nemovitosti, pozemky, stroje, ale také patenty, či obchodní značky. Do finančních řadíme peněžní prostředky, dluhopisy a akcie. Chápeme pojem aktiva?“ Pokud má žák dotaz, tak mu na něj odpovím.

Slide 4. „V dnešní době se setkáváme s pojmem kryptoměny, avšak správné označení je kryptoaktiva. Kryptoaktivum je typ nehmotné digitální měny. Klíčovým faktorem určující cenu kryptoaktiv jsou náklady na jejich získání. Kryptoaktiva se získávají za pomocí výpočetní technologie, která spotřebovává velké množství elektrické energie. Pro

lepší demonstraci Vám pustím toto video: https://www.mall.tv/kdo-to-plati/ohrozi-tezba-bitcoinu-nasi-planetu. Máme ke kryptoaktivum nějaké otázky?“ Pokud má žák dotaz, tak mu na něj odpovím.

30–38 Využití kryptoaktiv jako platebního nástroje

„Teď už víme, jak se určuje cena a na jaký hlavní faktor ovlivňuje cenu většiny kryptoaktiv. Pojďme se tedy podívat, jestli můžeme používat kryptoaktiva jako prostředníky směny, stejně jako peníze. Pro prostředek směny je důležité, aby všichni zúčastnění měli v prostředku směny užitek. Když jsem chodil na střední školu, tak jsme s přáteli hráli sběratelskou karetní hru Magic: The gathering, kde každá karta má svoji hodnotu. V praxi to vypadalo tak, že jsme byli schopni papírovou kartičku směnit s jiným sběratelem za peníze kvůli tomu, že obě strany dávali té dané kartě stejnou hodnotu. S kryptoaktivy je to hodně podobné, některé obchody kryptoaktiva přijímají jako platidlo. Těmito obchody jsou často restaurace, avšak u nás je to například i Alza.“

Slide 5. „V dnešní době v Česku přijímá stále více obchodů možnost placením kryptoaktivy, můžeme se podívat na stránku https://coinmap.org/, která tyto obchody eviduje.“

Slide 6. „Víte, jaká byla jedna z prvních věcí, která se koupila za bitcoin? Byla to pizza za 10 tisíc bitcoinů. Stalo se to tak, že jeden fanoušek bitcoinu napsal na fórum, že dá 10 tisíc bitcoinů tomu, kdo mu koupí pizzu. Jiný člen fóra přes telefon objednal pizzu přes telefon a zaplatil kartou. Kdybychom cenu pizzy přepočítali na dnešní hodnotu, tak ho vyšla na 2 miliardy korun. Máte nějaké otázky k využití kryptoaktiv jako platebního prostředku?“ Pokud má žák dotaz, tak mu na něj odpovím.

38–43 Shrnutí hodiny a rozdání studijní tabulky

„Dneska jsme toho stihli hodně, probrali jsme cenu, na základě nabídky a poptávky. Řekli jsme si, že cena výrobku by měla být větší, než jsou jeho náklady na výrobu a distribuci. Definovali jsme si, co je to aktivum a ukázali jsme si využití kryptoaktiv jako prostředku směny. Kvůli tomu, že jste dnes skvěle pracovali, jsem si pro Vás připravil studijní tabulku, ve které jsou shrnuté základní rozdíly peněz a kryptoaktiv.“

43–45 Rozdání dotazníků, zhodnocení vyučovací hodiny

„Jak se Vám dnešní hodina líbila? Chcete více prostoru v hodinách, pro vyjádření názorů? „Poprosím Vás, abyste mi na závěr vyplnili krátký anonymní dotazník.“ Poděkuji za dnešní hodinu a rozloučím se se třídou.

6.3 Struktura třetí hodiny ZSV

Název: Nákup a uchovávání kryptoaktiv

Charakteristika hodiny:

Hodina je zaměřena na kryptoaktiva. V první části hodiny si žáci zopakují vlastnosti kryptoaktiv. V druhé části hodiny se žákům dekonstruuje postup nákupu kryptoaktiv a jejich odeslání na hardwarovou peněženku. Na závěr hodiny jsou informace uceleny a sjednoceny. Vyučovací hodina učí žáka pracovat s kryptoaktivy.

Klíčová slova: kryptoaktiva, aktiva

Délka hodiny: 45 minut

Kontext hodiny:

Lekce bude probíhat ve třídě prvního ročníku čtyřletého gymnázia nebo v kvartě osmiletého gymnázia. Očekávaný věk žáků je 14-16 let. Tato hodina spadá v RVP G do kapitoly Člověk a svět práce, podkapitola Finance. Optimální počet žáků je dvacet čtyři. Je očekávána částečně odborná znalost tématu kryptoaktiva ze strany žáka. Tento předpoklad vyplývá z předchozích dvou hodin: Úvod do tématu měn, Kryptoaktiva a jejich hodnota.

Pomůcky:

- Tabule
- Křída nebo fix
- Projektor
- Připravená prezentace
- Sešit a psací potřeby
- Předpřipravenou studijní tabulku s rozdíly mezi penězi a kryptoaktivy
- Hardwarová peněženka

Cíle hodiny:

- Žák směňuje fiat měnu za kryptoaktiva
- Žák odesílá transakce pomocí kryptoaktiv

Klíčové kompetence:

- Kompetence k učení
- Komunikativní kompetence
- Kompetence k řešení problémů

Hodnocení:

Při hodině je hodnocena spolupráce žáků s vyučujícím a aktivita žáků během vyučovací hodiny. Hodnocení je slovní.

Uchování informací:

Žákům je umožněno zapisovat si poznámky a důležité informace do sešitů.

Časový harmonogram hodiny:

Časové rozmezí [min]	**Aktivita**
0–3	Úvod hodiny, seznámení žáků s průběhem hodiny
3–5	Motivace žáků ke zdravému přemýšlení o financích
5–15	Zopakování základních vlastností kryptoaktiv
15–23	Peněženky na kryptoaktiva
23-34	Nákup kryptoaktiv
34–38	Poslání kryptoaktiv na hardwarovou peněženku
38–43	Shrnutí hodiny a zpětná vazba
43–45	Rozdání dotazníků a předpřipravených listů, zhodnocení vyučovací hodiny

Tab. 7: Hodina ZSV 3 – vlastní tvorba

Popis aktivit:

Před začátkem hodiny

Vejdu do třídy a vítám příchozí žáky, abych je podpořil v dobrém zvyku chodit v čas. Tento čas před začátkem hodiny investuji do tvorby vztahu mezi mnou a žáky. Zajímám se o jejich názor a směji se jejich vtipům.

0–3 Úvod hodiny, seznámení žáků s průběhem hodiny

Poprosím žáky o ztišení. Přivítám žáky a seznámím je s průběhem hodiny: „Dneska probereme základní typy peněženek, na kterých se uchovávají kryptoaktiva, následně si ukážeme, jak se kryptoaktiva nakupují a jak probíhají jejich transakce."

3–5 Motivace žáků ke zdravému přemýšlení o financích

Začnu se žáky diskusi: „Viděli jste Tři veterány, pohádku podle předlohy Jana Wericha? V této pohádce se zpívá: „Není nutno, není nutno, aby bylo přímo veselo, hlavně nesmí býti smutno, natož aby se brečelo, chceš-li, trap se, že ti v kapse zlaté mince nechřestí, nemít žádné kamarády, tomu já říkám neštěstí". Co tím chtěl asi autor písně říct? Co je pro Vás důležitější než peníze?" Začínám diskusi se žáky, chci, aby si připomněli, že peníze nejsou vše. „Můj kamarád z Turecka mi vždy říkal: Pokud mám dost peněz na jídlo a bydlení, tak jsem bohatý."

5–15 Zopakování základních vlastností peněz a kryptoaktiv

Slide 1. „V minulých hodinách jsme probírali cenu kryptoaktiv, na konci hodiny jste dostali předpřipravenou studijní tabulku s rozdíly mezi penězi a kryptoaktivy, pokud ji někdo nemá, přinesl jsem jich pár navíc. Jaké znáte kryptoaktiva? Kde se s nimi můžete setkat? Jaké jsou vlastnosti většiny kryptoaktiv? K čemu se kryptoaktiva používají? Co určuje cenu kryptoaktiv? Kde se s nimi může platit?"

15–23 Peněženky na kryptoaktiva

Slide 2. „Možná si říkáte, proč jsem pro slide o softwarových peněženkách zvolil tento obrázek. Tímto obrázkem jsem chtěl demonstrovat různé typy peněženek pro kryptoaktiva. Základními pěti typy peněženek jsou softwarové, onlinové, mobilní, papírové a hardwarové. Softwarová peněženka je program, který si stáhnete do počítače. Tento program Vám vygeneruje peněženku, na kterou můžete ukládat svá kryptoaktiva. Tato peněženka je bezpečná podle toho, jak bezpečný je váš počítač. Druhým typem je online peněženka, i když tady označení peněženka není moc vhodný, protože se jedná o

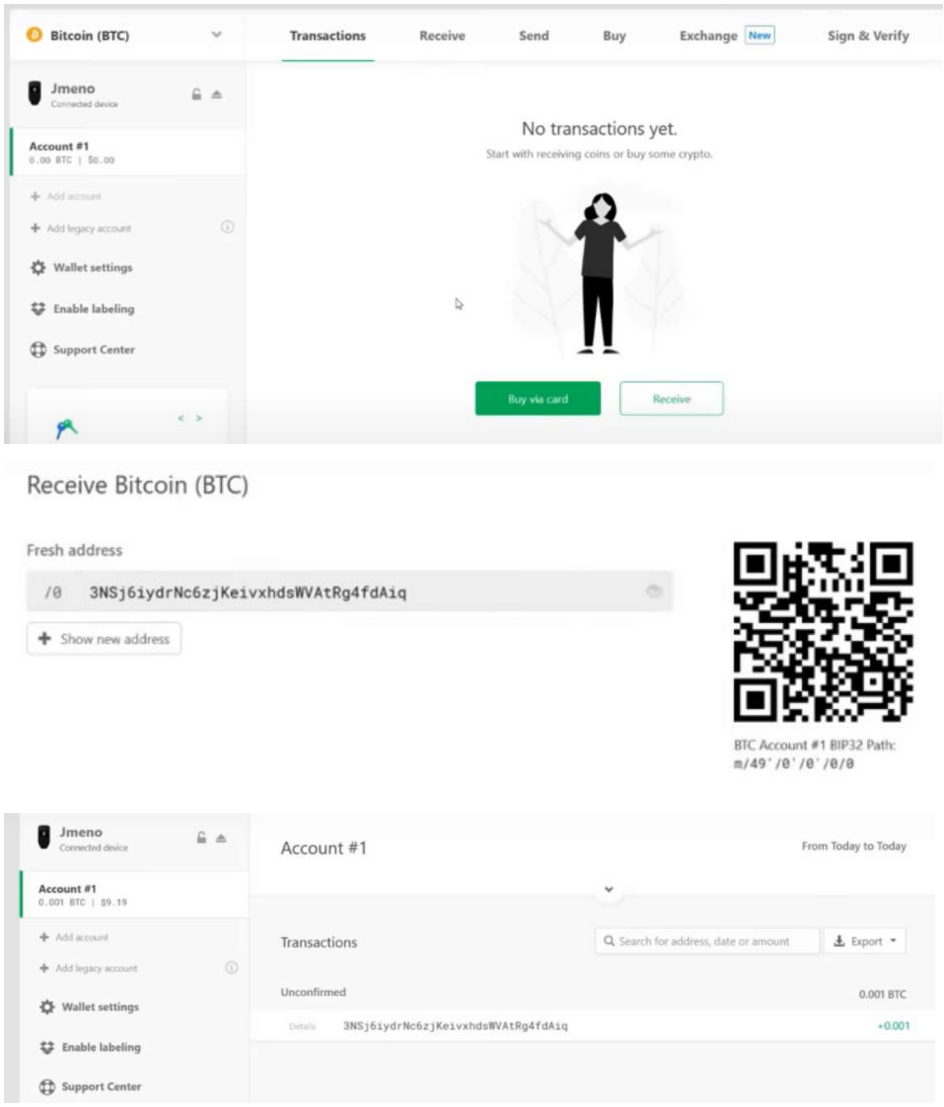
způsob, kdy jsou kryptoaktiva uschována na učtu, který se zpravidla nachází na internetové burze. Tento způsob úschovy kryptoaktiv je sice nebezpečný, nicméně jeho výhoda oproti ostatním peněženkám je možnost rychlého směňování kryptoaktiv za jiná. Třetí typ peněženky je mobilní, která je zlatým středem mezi softwarovou a online peněženkou, co se týká přenosnosti a bezpečí. Jedná se o aplikaci, kterou si stáhnete do svého smartphonu, která vám umožní na ni uchovávat svá kryptoaktiva, takže je máte pořád k dispozici. Čtvrtým typem je papírová, s tou se můžete setkat v bitcoin bankomatech. Tato peněženka je velmi bezpečná, protože není připojená k internetu, na druhou stranu může jednoduše dojít k jejímu poškození. Poslední typem peněženek je hardwarová, kterou jsem Vám přinesl ukázat. Ano, vypadá jako flash disk, nicméně v sobě uchovává adresu, na kterou si mohu ukládat svá kryptoaktiva. Máte k peněženkám pro kryptoaktiva nějaké otázky?“ Pokud má žák dotaz, tak mu na něj odpovím.

23-34 Nákup kryptoaktiv

„Kryptoaktiva nemusíte pouze těžit, ale můžete je směnit za peníze, nejčastěji pomocí nějaké burzy.“ Slide 3. „Nejjednodušší způsob, kdybyste si chtěli nakoupit kryptoaktiva, je poslat si peníze z banky rovnou na burzu a tam peníze směnit za kryptoaktiva. Když já nakupuji kryptoaktiva, tak používám revolut, k směně jedné měny za druhou, kvůli lepšímu kurzu. Znáte revolut? Je to debetní karta, která umožňuje směnu měn. V jejím samotným prostředí najdete směnu za kryptoaktiva, nicméně to má jeden háček. Pokud si tam směníte své peníze za kryptoaktiva, tak budete držet aktivum o hodnotě toho daného kryptoaktiva, ale ne to kryptoaktivum samotné. Co to v praxi znamená? Vámi získaná kryptoaktiva přes revolut nemůžete posílat dalším lidem, vy nevlastníte kryptoaktivum, ale pouze aktivum o hodnotě daného kryptoaktiva. Přirovnal bych vám to k autorským právům u DVDček, u nich také vlastníte myšlenku a provedení filmu, ale nevlastníte práva k film. Máte k nákupu kryptoaktiv nějaké otázky?“ Pokud má žák dotaz, tak mu na něj odpovím. „Dobře, teď jsme si to probrali teoreticky. A teď se podíváme, jak to vypadá v praxi.“ Pustím video a průběžně ho komentuji: https://www.youtube.com/watch?v=-8uLLuvCqvM&t=635s . „Dalším způsobem, jak si koupit kryptoaktiva je pomocí krypto bankomatů.“ Slide 4. Otevírám odkaz: https://coinatmradar.com/country/57/bitcoin-atm-czech-republic/ a ukazuji žákům hustotu bankomatů, ve kterých si lze koupit kryptoaktiva.

34–38 Poslání kryptoaktiv a na hardwarovou peněženku

Slide 5. „Když už jsme si kryptoaktiva nakoupili, tak si ještě ukážeme, jak si je převést na svoji peněženku. Burza vám nabídne možnost odeslání kryptoaktiv, jak vidíte na obrázku. Ve své peněžence si kliknete na tlačítko obdržet, peněženka Vám následně vygeneruje adresu, na kterou máte kryptoaktiva poslat, nejčastěji formou QR kódu.“ Demonstruji tento postup žákům na hodině.



Obr. 16: Způsob pomocí QR kódu – vlastní tvorba

38–43 Shrnutí hodiny a zpětná vazba

„Dneska jsme si řekli o různých typech peněženek pro kryptoaktiva a ukázali jsme si prakticky, jak se dají kryptoaktiva nakoupit a uschovat. Jak se vám dnešní hodina líbila? Vidíte nějaký zásadní rozdíl mezi posíláním peněz pomocí internetového bankovnictví a pomocí kryptoaktiv? Byla pro Vás hodina srozumitelná? “

43–45 Rozdání dotazníků, zhodnocení vyučovací hodiny

„Dneska jste byl klidní, je vidět, že vám problematika kryptoaktiv zajímala, co byste se chtěli o kryptoaktivech ještě dozvědět? Poprosím Vás, abyste mi na závěr vyplnili krátký anonymní dotazník.“ Poděkuji za dnešní hodinu a rozloučím se se třídou.

Závěr

Tato bakalářská práce měla v první řadě za cíl poskytnout vhled do problematiky kryptoměn a poukázat na vhodnost jejího zařazení do Rámcového vzdělávacího programu pro gymnázia (RVP G). V rámci teoretické části této práce proto byla věnována pozornost pojmům, jako je RVP G, peníze, kryptoaktiva a blockchain. Jelikož původní záměr spočíval v zaměření praktické části na šetření v rámci vyučovacích hodin, bylo nezbytné zabývat se v teoretické části i metodami vyučování.

Kapitola *3.4 Využití blockchainu*, jež je součástí teoretické části, stojí za povšimnutí, jelikož je v ní zdůrazněn široký prostor pro využití technologií kryptoaktiv, které pomáhají zefektivnit finanční toky, zdravotnictví, logistiku, energetiku, pojišťovnictví. Zajímavým poznatkem je též fakt, že díky smart contractům můžeme v budoucnosti zautomatizovat smlouvy a tím ulehčit byrokracii systému.

Jak již bylo výše zmíněno, praktická část se měla opírat o vyučovací hodiny. Ty se však z důvodu pandemie COVID-19 nemohly uskutečnit.

Očekávaný výsledek odučených modelových hodin měl ukázat rostoucí zájem žáků o znalosti této technologie. Přestože se žáci s těmito pojmy pravděpodobně ve svém volném čase setkali, neočekává se hlubší znalost této technologie, jelikož je složitá na pochopení. Tento předpoklad je jedním z hlavních důvodů, proč by se mělo téma kryptoaktiv zařadit do RVP. Tím by se doplnily znalosti žáků v oblastech decentralizovaných aplikací, decentralizovaných databází, vlastností kryptoaktiv, těžby kryptoaktiv, vlastností blockchainu a jeho využití.

Žáci by nabyté znalosti využili v praktickém životě při ukládání informací do decentralizovaných databází, využívali by kryptoaktiva i jako novou formu peněz, která však oproti bankám nevyžaduje soukromé údaje uživatele. Rovněž by žáci mohli kryptoaktiva použít při investičních příležitostech.

Česká republika by se tak stala další zemí, stejně jako Francie, která by zařadila kryptoaktiva do rámcově vzdělávacího programu. (Petráš, 2019).

Závěr této bakalářské práce měl otevřít diskuzi o zařazení tématu kryptoaktiva do RVP G.

Během psaní této bakalářské práce a COVID pandemie, začala firma MasterCard, oslavovat firmy zabývající se kryptoaktivy s nabídkou tvorby debetních karet pro kryptoaktiva pod jejich hlavičkou (Huillet, 2020), to potvrzuje rostoucí zájem o tuto technologii.

Seznam použité literatury

BALADA, Jan; et.al. 2007. *Rámcový Vzdělávací Program pro Gymnázia RVP G*.

BAKER, Jessi. 2013. "A Platform and Consultancy for Transparency." *Provenance*. Retrieved (https://www.provenance.org/about).

BERTL, Ivan. 2018. *Finanční gramotnost: otázky a odpovědi, problémy a jejich řešení*. V Ústí nad Labem: Univerzita J.E. Purkyně, Pedagogická fakulta, 2018. ISBN 978-80-7561-134-5.

Bitcointalk. 2009. "Bitcoin Forum." Retrieved (https://bitcointalk.org/).

Blockbase Mining. 2020. "Cryptocurrency Mining Glossary." Retrieved (https://blockbasemining.com/glossary).

Blockgeeks. 2019. "What Are Dapps? The New Decentralized Future." Retrieved (https://blockgeeks.com/guides/dapps/).

Blockchain.com. 2020. "Celková Míra Hašování." Retrieved (https://www.blockchain.com/charts/hash-rate).

Bohemiasoft. 2017. "Stavíme RIG pro Těžbu Etherea." Retrieved (https://blog.webareal.cz/stavime-rig-pro-tezbu-etherea-1-dil/?fbclid=IwAR2OICPL6McCL6S3J50Eq5p46dQR4bcMRtuD5wD6211fYVdbRMAW4ghOGnU).

BOŘÁNEK, Roman. 2014. "Czech Crown Coin: Český Pokus O Národní Kryptoměnu." *Root.cz*. Retrieved (https://www.root.cz/clanky/czech-crown-coin-cesky-pokus-o-narodni-kryptomenu/?fbclid=IwAR1mkYerM57fzJq8qD-XWso6j66_WD8lQMPxq4K0JWA-iDmA18iX8doCRf8).

BUTERIN, Vitalik. 2013. "Ethereum." Retrieved (https://ethereum.org/).

CERVENKA, Andreas. *Peníze: jakou mají cenu?*. Praha: Práh, 2014, 129 s. ; 19 cm. ISBN 978-80-7252-504-1.

European Central Bank. 2012. *Virtual Currency Schemes*.

EYAL, Ittay; et. al. 2014. "Majority Is Not Enough: Bitcoin Mining Is Vulnerable." *Department of Computer Science, Cornell University, Ithaca, USA* 436.

FERGUSON, Niall. *Vzestup peněz: finanční dějiny světa*. Praha: Argo, 2011. Historické myšlení. ISBN 978-80-257-0337-3.

FILLNER, Karel. 2014. "Vlastnosti Btc, Výhody I Nevýhody." *Btctip*. Retrieved (https://btctip.cz/vlastnosti-btc-vyhody-i-nevyhody/?fbclid=IwAR30u859KTnzbonNiue8a5cLYq6Nok2oyAVXdN2RK7te7vg6lRLToYG3I8g).

FINEX. 2020. "Kryptoměnové Peněženky - Jak Vybrat Tu Správnou?" Retrieved (https://finex.cz/rubrika/kryptomeny/penezenky/?fbclid=IwAR1DMcSVhFw4xgS9wmCHg-_i_vbCKFQy6ztNGwDO1YeMYCcIc4RAbuGfQQQ).

FRANKENFIELD, Jake. 2020. "Cryptocurrency." *MICHAEL SONNENSHEIN*. Retrieved (https://www.investopedia.com/terms/c/cryptocurrency.asp).

HOSKINSON, Charles. 2015. "Cardano." *IOHK*. Retrieved (https://iohk.io/en/about/).

HŘIVNA, Jan. 2018. "Technologie Blockchain a Její Využití." Vysoká škola ekonomická v Praze.

HUILLET, Marie. 2020. "Mastercard Expands Cryptocurrency Program for Crypto Card Issuers" Retrieved (https://cointelegraph.com/news/mastercard-expands-cryptocurrency-program-for-crypto-card-issuers).

JAVŮREK, Karel. 2018. "Před Deseti Lety Vznikl Bitcoin. Co Se Vlastně Tenkrát Stalo?" *Connect*. Retrieved (https://connect.zive.cz/clanky/bitcoin-vznikl-v-roce-2008/sc-320-a-194622/default.aspx?fbclid=IwAR252PkjbHcBDyO7GG2th9lqj9LHbTqmszHQmjypadIPPl1HOoPr6f-MVTM).

Jrcornel. 2018. "Bitcoin Is like the Internet in the 1980's." *Steemit*. Retrieved (https://steemit.com/bitcoin/@jrcornel/bitcoin-is-like-the-internet-in-the-1980-s).

Junior Achievement. 2000. "Interní Materiál K Řízení Vyučovací Jednotky." *Praha*.

JUŘÍK, Pavel. 2012. *Platební karty: ilustrovaná historie placení*. Praha: Libri, 2012. ISBN 978-80-7277-498-2.

JŮVA, Vladimír. 1983. "Úvod Do Pedagogiky a Psychologie pro Učitele." Brno.

KALISKÝ, Boris. 2018. *Bitcoin a ti druzí: nepostradatelný průvodce světem kryptoměn*. [Praha]: IFP Publishing, 2018. ISBN 978-80-87383-71-1.

KLEIN, Michelle. 2020. “WHAT’S THE DIFFERENCE BETWEEN CPU AND GPU MINING?” *Bite My Coin*. Retrieved (https://bitemycoin.com/cryptocurrency-mining/whats-the-difference-between-cpu-and-gpu-mining/?fbclid=IwAR2j3DmxbSRf2dTkiQbo-ixnw4uijoD0oESRXqk4mrA1vVf5ZVNJ-PLo0Ps).

KRPÁLEK, Pavel; et. al. 2012. “Metodický Materiál K Realizaci Řízené Pedagogické Praxe Na Fakultních Školách Vysoké Školy Ekonomické v Praze. Výstup Z Projektu FRVŠ Č. 1310/2012 Inovace Předmětu „Řízená Pedagogická Praxe“ v Bakalářském Studijním Programu Učitelství Na Katedře Didaktiky.” *ExtraSYSTEM* 12.

LEE, Charlie. 2011. “Litecoin.” *THE FUTURE OF MONEY*. Retrieved (https://litecoin.com/en/).

LEONARD, Christopher. 2020. “How Jay Powell’s Coronavirus Response Is Changing the Fed Forever.” *TIME*. Retrieved (https://time.com/5851870/federal-reserve-coronavirus/).

Limited, TETHER. 2018. “Attorney-Client Communication/Work Product Privileged & Confidential.” Retrieved (https://tether.to/wp-content/uploads/2018/06/FSS1JUN18-Account-Snapshot-Statement-final-15JUN18.pdf).

MAŇÁK, Josef. 2001. “Funkce Metod ve Výuce.” *Metody Tvořivého Učitele – Pedagogická Orientace* 3.

MAŇÁK, Josef a Vlastimil ŠVEC. *Výukové metody*. Brno: Paido, 2003, 219 s. : il. ; 23 cm. ISBN 80-7315-039-5.

MAZÁČOVÁ, Nataša. 2014. “Didaktiky, Vybrané Problémy Obecné.” Univerzita Karlova.

Ministerstvo školství, mládeže a tělovýchovy. 2016. *Opatření Ministryně Školství, Mládeže a Tělovýchovy, Kterým Se Mění Rámcový Vzdělávací Program pro Gymnázia, Rámcový Vzdělávací Program pro Gymnázia Se Sportovní Přípravou a Rámcový Vzdělávací Program pro Dvojjazyčná Gymnázia – Pilotní Verze a Rámcový Vzd*.

Mt.Gox. 2018. “7 of the Biggest Recent Hacks on Crypto Exchanges.” Retrieved (https://www2.cso.com.au/article/635648/7-biggest-recent-hacks-crypto-exchanges/).

NAKAMOTO, Satoshi. 2008. “A Peer-to-Peer Electronic Cash System. In: Bitcoin.” *[Online]*.

NARAYANAN, Arvind; et. al. 2016. *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*.

PALATINUS, Marek (A). 2020. “Trezor.” *Satoshilabs*. Retrieved (https://wallet.trczor.com/#/).

PALATINUS, Marek (B). 2020. “Slush Pool.” *Satoshilabs*. Retrieved (https://slushpool.com/home/?fbclid=IwAR2ZF_76AioY6tJaZ5hPwYFXYaghb7L8Eopeg2WvrNB0fJ1DkdRY9QOJ_0c&__cf_chl_jschl_tk__=0bd00164c1c4466d0b907f919e1a2498117c6cd3-1589289896-0-AdSwEsbLOKMaiLO0CE7znz7jhjXHnAcfE1KJFIQpTj2F89H2Y5CAUm2N-6d7VNXHwjwUF1fYh2vlQOB9pPn9).

Pando LO3energy. 2018. “Engage Customers, Enable Green Communities and Reshape Our Energy Future.” Retrieved (https://lo3energy.com/pando/).

PAPERNO, Alex. 2017. “Teambrella: A Peer-to-Peer Coverage System.” *Teambrella*. Retrieved (https://teambrella.com/whitepaper.pdf).

Paymium. 2020. “Obchodujte Kryptoměny S Finanční Pákou.”

PETRÁŠ, Radek. 2019. “Francouzské střední školy budou učit o Bitcoinu a kryptoměnách“ Retrieved (https://kryptomagazin.cz/francouzske-stredni-skoly-budou-ucit-o-bitcoinu-a-kryptomenach/)

REVENDA, Zbyněk. 2012. *Peněžní ekonomie a bankovnictví*. 5., aktualiz. vyd. Praha: Management Press, 2012. ISBN 978-80-7261-240-6.

TASSEV, Lubomir. 2019. “The Number of Cryptocurrency Wallet Users Keeps Rising.” *Bitcoin.com*. Retrieved (https://news.bitcoin.com/the-number-of-cryptocurrency-wallet-users-keeps-rising/).

ROTHBARD, Murray Newton. 2001. *Peníze v rukou státu: jak vláda zničila naše peníze*. Praha: Liberální institut, c2001. ISBN 80-86389-12-X.

RUBARIO, Steve 2020. “Best Bitcoin Mining Pools 2020 – The Ultimate List of Mining Pools.” *Bitcoin Mining*. Retrieved (https://www.bitcongress.org/bitcoin/mining/best-bitcoin-mining-pools/).

RUDDEN, Jennifer. 2020. “Bitcoin Price Index from July 2012 to May 2020.” *Statista*. Retrieved (https://www.statista.com/statistics/326707/bitcoin-price-index/).

SASSEN, Gerard. 2017. “DeadCoins.com: Seznam Více Než 600 Mrtvých Kryptoměn a Kryptoaktiv.” *Bitcoinblog.cz*. Retrieved (https://bitcoinblog.cz/deadcoins-com-aneb-vice-nez-600-mrtvych-kryptomen-a-kryptoaktiv/?fbclid=IwAR3pyQv9HWx8_wyt0ZHHRLA25YKNF54fS4vXPh49M2H9g5Afu-mdXRNQ-lg).

SCHLOSSBERGER, Otakar. 2012. *Platební služby*. Praha: Management Press, 2012. ISBN 978-80-7261-238-3.

SEDGWICK, Kai. 2002. *Everything You Should Know About Bitcoin Address Formats*.

SHIRRIFF, Ken. 2019. “Bitcoin Mining the Hard Way: The Algorithms, Protocols, and Bytes.” *Righto*. Retrieved (http://www.righto.com/2014/02/bitcoin-mining-hard-way-algorithms.html?fbclid=IwAR3C-pqKfH2N6vuBXB_dud9bOos5Pwfu8oX_O6FOYLpImdcdp8dnP25PT-k).

STARR, Ross M. 1989. *Money and the Mechanism of Exchange*.

STROUKAL, Dominik a Jan SKALICKÝ. 2018 *Bitcoin a jiné kryptopeníze budoucnosti: historie, ekonomie a technologie kryptoměn, stručná příručka pro úplné začátečníky*. 2., rozšířené vydání. Praha: Grada Publishing, 2018. Finance pro každého. ISBN 978-80-271-0742-1

ŠVARCOVÁ, Jena. *Ekonomie: stručný přehled : teorie a praxe aktuálně a v souvislostech : učebnice : [2013/2014]*. Zlín: CEED, 2013. ISBN 978-80-87301-17-3.

VEBER, Jaromír 2018. *Digitalizace ekonomiky a společnosti: výhody, rizika, příležitosti*. Praha: Management Press, 2018. ISBN 978-80-7261-554-4

Seznam zkratek

NVP	Národní vzdělávací program
RVP	Rámcový vzdělávací program
RVP G	RVP pro gymnázia
RPSN	Roční průměrná sazba nákladů
ČNB	Česká národní banka
NB	Národní banka
tzn.	To znamená
ICT	Informační a komunikační technologie
RAM	Random Access Memory
P2P	Peer to peer
P2PKH	Pay to PubKey Hash
CPU	Central processing unit
GPU	Graphics processing unit
Kč	Koruna česká
ETH	Ethereum
ČR	Česká republika
ASIC	Application Specific Integrated Circuit
GB/s	Gigabite za sekundu
DLT	Decentralizované aplikace
USD	Americký dolar
NFC	Near field Communication
IVP	Individuální vzdělávací plán

Seznam grafů

Seznam obrázků

Seznam tabulek

Seznam příloh

Příloha 1	Tabulka Peníze a Bitcoin
Příloha 2	Tabulka Dotazník
Příloha 3	Prezentace IVT2
Příloha 4	Prezentace IVT3
Příloha 5	Prezentace ZSV1
Příloha 6	Prezentace ZSV2
Příloha 7	Prezentace ZSV3
Příloha 8	Procvičovací list pro první modelovou hodinu IVT
Příloha 9	Test na druhou modelovou hodinu Informatiky

Přílohy

Příloha 1: Předpřipravenou studijní tabulku s rozdíly mezi penězi a kryptoaktivy

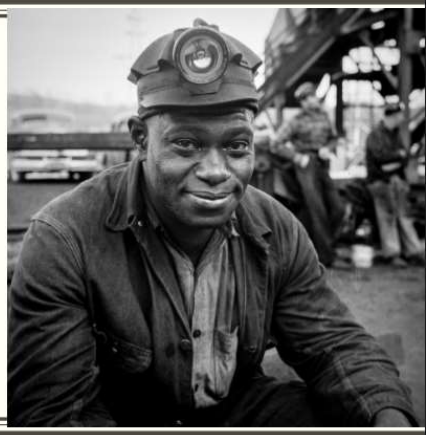
	Peníze	Kryptoaktiva
Vytvořeny lidmi?	Ano	Ano
Slouží jako prostředek směny?	Ano	Ano
Dělitelnost?	Ano	Ano
Skladovatelnost?	Ano	Ano
Co dokládá jejich hodnotu?	Kdysi zlato	Spotřebovaná elektrika
Centrální autorita?	Ano	Ne (Decentralizované)
Fyzické?	Ano	Ne,
Digitální?	Ano	Ano
Anonymní?	Ne	Ano
Společenská akceptovatelnost?	Ano, všude	Ano, vyjímečně
Náročné na pochopení?	Ano	Ano, velmi

Příloha 2: Dotazník

Anonymní zpětná vazba na proběhlou vyučovací hodinu						
Pohlaví		Muž		Žena		
Dostáváte kapesné		Ano		Ne		
	Hodnocení 1-nejlepší/často/ano; 5-nejhorší/nikdy/ne					
1.	Jak se ti hodina líbila?	1	2	3	4	5
2.	Přišla ti hodina zajímavá	1	2	3	4	5
3.	Byla hodina srozumitelná?	1	2	3	4	5
4.	Měl/a jsi dostatek prostoru na dotazy?	1	2	3	4	5
5.	Jak často se ve svém volném čase zajímáš o moderní technologie?	1	2	3	4	5
6.	Jak na sebe navazovali informace během hodiny?	1	2	3	4	5
7.	Setkal/a jsi se již s termínem kryptoaktiva?	1	2	3	4	5
8.	Zajímá tě tématika kryptoaktiv?	1	2	3	4	5
9.	Setkal/a jsi se již s pojmem blockchain?	1	2	3	4	5
10.	Zkoušel/a jsi těžit kryptoaktiva?	1	2	3	4	5
11.	Znáš někoho, kdo zkoušel těžit kryptoaktiva?	1	2	3	4	5
12.	Vlastníš nějaké kryptoaktiva?	1	2	3	4	5
13.	Znáš někoho, kdo vlastní kryptoaktiva?	1	2	3	4	5
14.	Přinesla ti hodina nové informace?	1	2	3	4	5
15.	Ocenil/a bys další hodiny na téma kryptoaktiva?	1	2	3	4	5
16.	Jak bys vylepšil tuto hodinu?					
	Ve svém volném čase za zajímám o moderní technologie					

Příloha 3: Prezentace IVT2

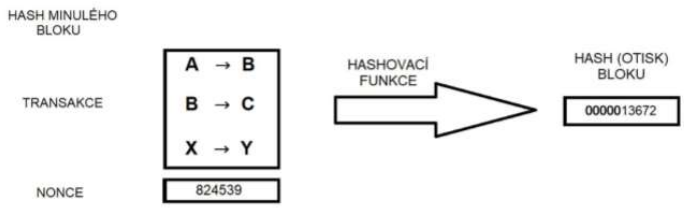
PRINCIP TĚŽBY KRYPTOAKTIV



KRYPTOAKTIVA

Tato fotka od autora Neznámý autor s licencí CC BY-SA

BLOCKCHAIN



TĚŽAŘOVA VÝHODA NAD KONKURENCÍ

- Větší výpočetní výkon
- Levnější elektrika

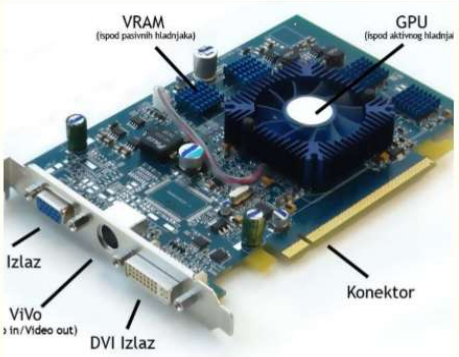
https://www.mall.tv/kdo-to-plati/ohrozi-tezba-bitcoinu-nasi-planetu

---

DĚKUJI ZA POZORNOST

Příloha 4: Prezentace IVT3

GRAFICKÉ KARTY A ASIC ZAŘÍZENÍ



GRAFICKÁ KARTA - definice

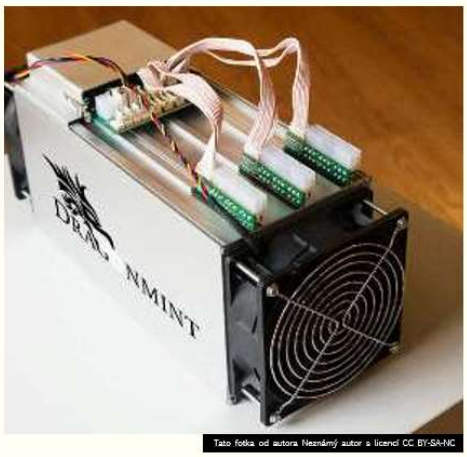
„Stará se o vykreslení obrazu na monitor.“

GRAFICKÁ KARTA - komponenty

- Integrovaný procesor - GPU
- Operační paměť
- Napájecí kaskáda
- Chlazení
- Výstupy
- Komunikační sběrnici

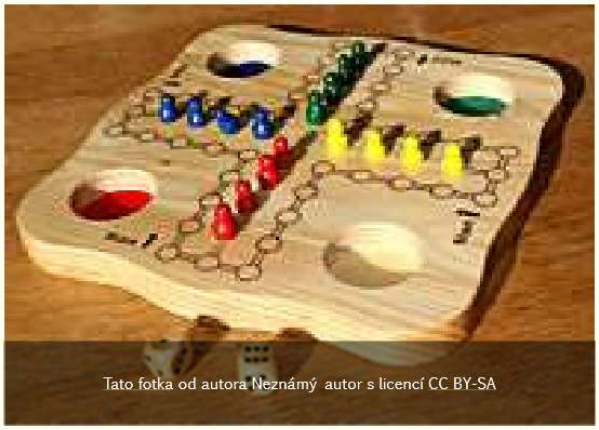
ASIC

- *„Application Specific Integrated Circuit“*
- Integrovaný obvod pro konkrétní aplikaci
- Nejčastější využití: Těžba kryptoaktiv



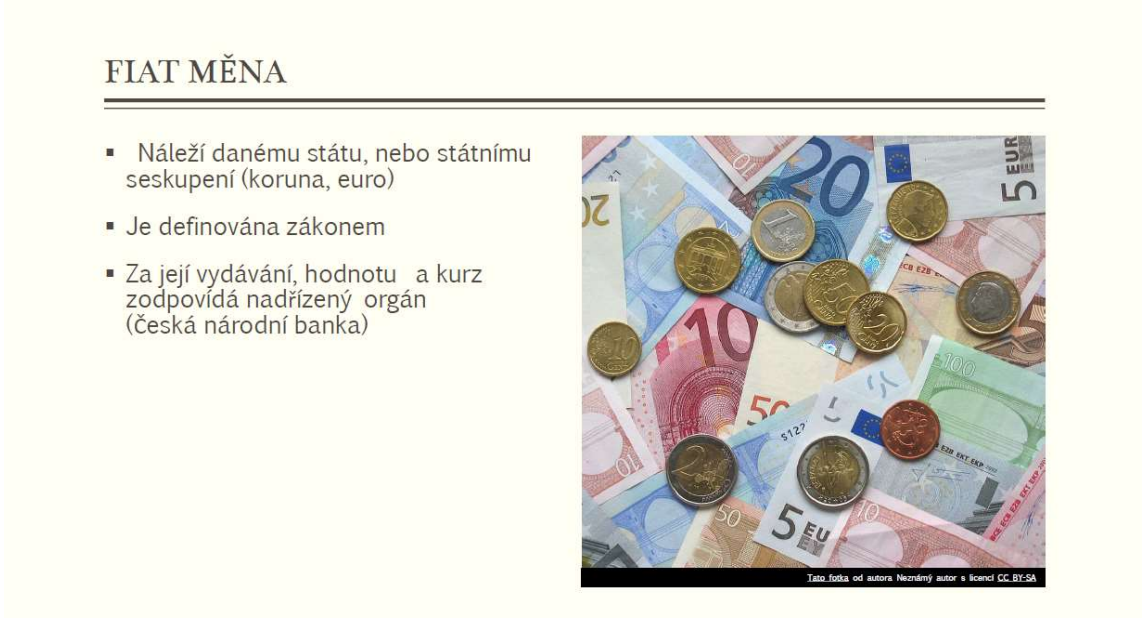
TĚŽBA KRYPTOAKTIV

TĚŽBA KRYPTOAKTIV – teorie her



DĚKUJI ZA POZORNOST

Příloha 5: Prezentace ZSV1



DIGITÁLNÍ MĚNA

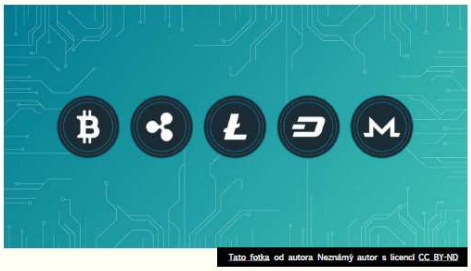
- Digitalizovaná forma peněz
- Internetové bankovnictví

VIRTUÁLNÍ MĚNA

- Virtuální platidlo
- Používá se v určitých komunitách
- Nejčastěji se získává směnou za reálné peníze
- Většinou mají regulovaný tok, nedají se směnit zpět na reálné peníze
- Zlaťáky, rubíny, mince, Riot points

KRYPTOMĚNA

- Správný název kryptoaktivum
- Používá se v určitých komunitách
- Peer-to-peer (P2P), decentralizované, pseudoanonymní



DĚKUJI ZA POZORNOST

Příloha 6: Prezentace ZSV2

CENA A AKTIVA

CENA - Nabídka a poptávka

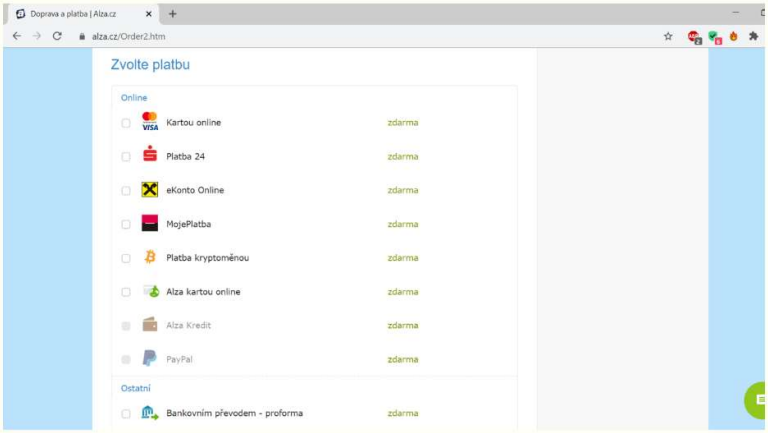
AKTIVUM

- Aktivum obecně chápeme jako něco, co přináší vlastníkovi nějaký výnos, nebo se očekává, že ho přinese v budoucnu.
- Aktiva reálná a finanční.
- Reálná aktiva - nemovitosti, pozemky, stroje, patenty a obchodní značky.
- Finanční aktiva - peněžní prostředky, dluhopisy a akcie.

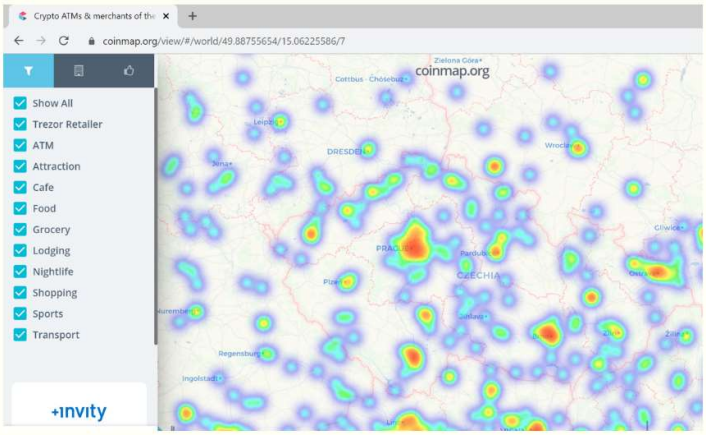
KRYPTOAKTIVA

- https://www.mall.tv/kdo-to-plati/ohrozi-tezba-bitcoinu-nasi-planetu

PLATBY KRYPTOAKTIVY



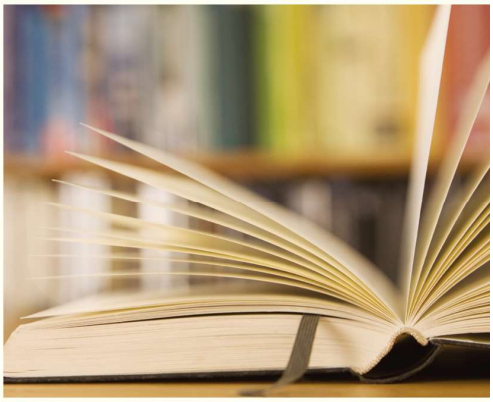
COINMAP



DĚKUJI ZA POZORNOST

Příloha 7: Prezentace ZSV3

NÁKUP A UCHOVÁVÁNÍ KRYPTOAKTIV



TYPY PENĚŽENEK PRO KRYPTOAKTIVA

- Softwarová peněženka
- Online peněženka
- Mobilní peněženka
- Papírová peněženka
- Hardwarová peněženka

NÁKUP KRYPTOAKTIV

Banka -> Burza

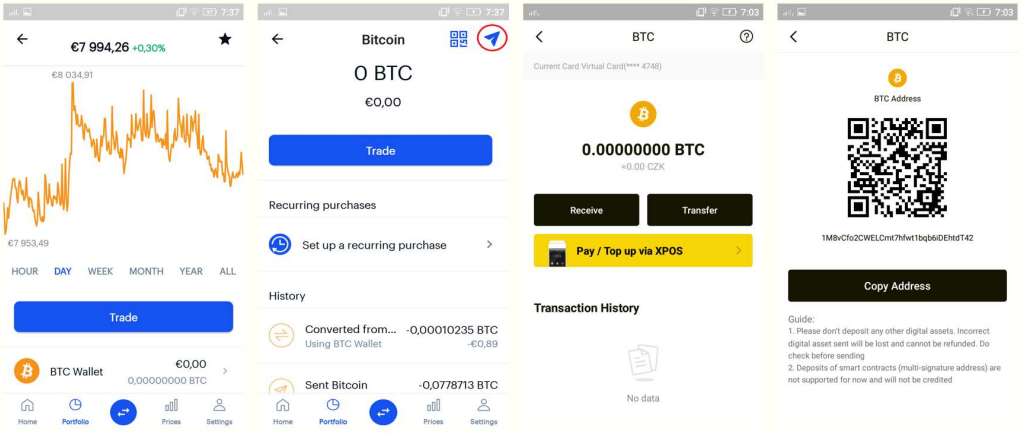
Banka -> Revolut -> Burza

https://www.youtube.com/watch?v=-8uLLuvCqvM&t=635s

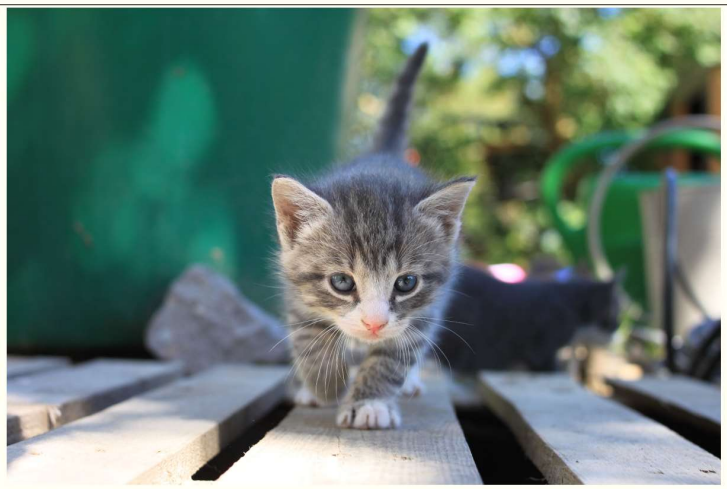
BANKOMAT NA KRYPTOAKTIVA

- https://coinatmradar.com/country/57/bitcoin-atm-czech-republic/

ÚSCHOVA KRYPTOAKTIV

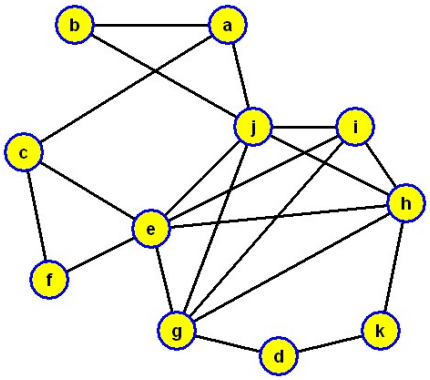


DĚKUJI ZA POZORNOST



Příloha 8: Procvičovací list pro první modelovou hodinu IVT

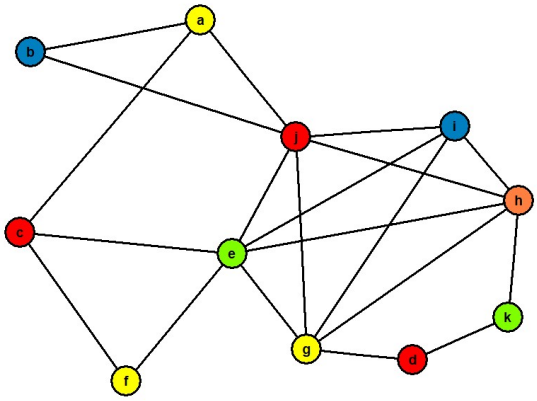
U následujících dvou grafů **rozhodněte a zdůvodněte**, zda daný graf je nebo není bipartitiní, a určete barevnost každého z daných grafů.



Řešení:

Graf není bipartitní, neboť obsahuje kružnici liché délky C5 = (j, i, h, g, e, j)

Barevnost grafu je 5 (dáno úplným grafem C5)



Příloha 9: Test na druhou modelovou hodinu Informatiky

1. **Definuj pojmy:**

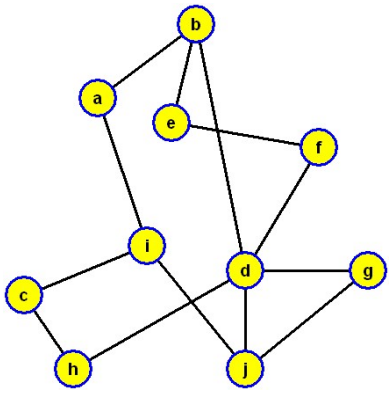
   - **Strom grafu**
   - **Kružnice grafu**
   - **Hrana grafu**
   - **Stupeň vrcholů**

2. **Vyvraťte tvrzení:**

$\forall_{G=(V,E)}$ graf G je bipartitní graf $\Rightarrow$ graf G neobsahuje most

$\forall_{G=(V,E)}$ graf G je bipartitní graf $\Rightarrow$ graf G obsahuje most

3. **U následujícího grafu rozhodněte, zda je graf bipartitiní a určete barevnost grafu. Své rozhodnutí zdůvodněte.**



Doplňková otázka: Na jakém principu funguje Caesarova šifra?

Správné řešení:

1. **Definuj pojmy:**

Strom grafu – Souvislý graf, který neobsahuje kružnici, nazýváme stromem.

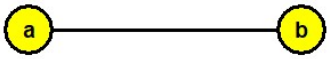
Kružnice grafu – Cesta délky, ve kterém je **první a poslední vrchol stejný.**

Hrana grafu – Nechť e = {v, w} je hrana grafu G. Vrcholy v, w nazýváme koncovými vrcholy hrany e.

Stupeň vrcholů - Stupeň vrcholu v, v grafu G, je číslo rovnající se počtu hran z vrcholu v.

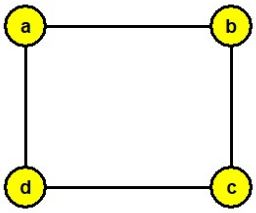
2. **Vyvraťte tvrzení:**

$\forall_{G=(V,E)}$ graf G je bipartitní graf $\Rightarrow$ graf G neobsahuje most
$\exists_{G=(V,E)\ \text{graf}}$ G je bipartitní graf $\wedge$ graf G obsahuje most

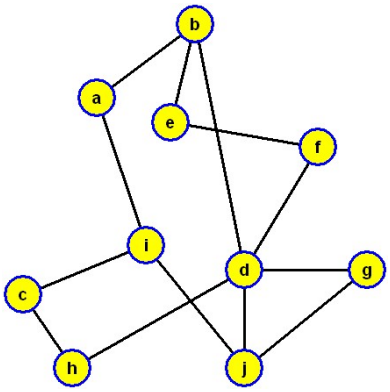


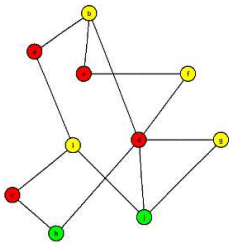
$\forall_{G=(V,E)}$ graf G je bipartitní graf $\Rightarrow$ graf G obsahuje most

$\exists_{G=(V,E)\ \text{graf}}$ G je bipartitní graf $\wedge$ graf G neobsahuje most



3. **U následujícího grafu rozhodněte, zda je graf bipartitiní a určete barevnost grafu. Své rozhodnutí zdůvodněte.**





Graf G_1 není bipartitní, neboť obsahuje kružnice liché délky C3 = (d, g, j, d)

Barevnost grafu je 3 (dáno úplným grafem C3)

4. ***Doplňková otázka*** **–** Na jakém principu funguje Caesarova šifra?
   Caesarova šifra funguje na principu, záměny (posunu) znaků.

   Např: A → B, B → C...