MUNI
LAW

Smart contracts, blockchain, kryptoměny

František Kasl

ÚPT PrF MU

7.3.2021

Disclaimer

- Tato prezentace je určena pro potřeby studijního programu MU LI302Zk Právo e-commerce.
- Prezentované názory jsou názory autora, nikoliv instituce, se kterou je afiliován.
- Hypertextové odkazy skrývající se pod vyznačenými pojmy v rámci prezentace směřují ke zdrojům informace či doplňkovým materiálům, které poskytují konkrétní příklady či bližší pojednání o daném pojmu. Přístup k těmto materiálům je na uvážení studujících.

Obsah

MUNI
LAW

Úvod a vymezení pojmů

Rámování problematiky skrze pojmy

Implikace regulatorního rámce dána již vlastním označením

- **Kryptoaktiva X Kryptoměny/Virtuální měny X Kryptoderiváty**

Společné prvky

- **Využití kryptografie + distribuovaná správy záznamů** (*distributed ledger technology* = *DLT*)

Množství forem a použití

- nástroj směny = digitální měna
- nástroj zpřístupnění služby = token na služby (*utility token*)
- investiční nástroj
- kombinace

Rámování problematiky skrze pojmy

- **Blockchain vs. DLT**
- **Kryptoaktiva vs. kryptoměny**
- **Smart kontrakty**

- **Virtuální povaha** – problém jurisdikce / povaha věci / zdanění transakcí / regulace a zabránění nelegálním transakcím / zabezpečení a standard ochrany uživatelů a investorů
- **Transformativní element** - nové role finančních zprostředkovatelů, nové ekonomické modely, nové regulatorní přístupy, potřeba mezinárodní spolupráce

Kontroverzní povaha kryptoaktiv

Proponenti

- revoluce platebních služeb, vyšší bezpečnost skrze nezměnitelnost, P2P infrastruktura pro levné přeshraniční transakce, transparentnost, nezávislost na politické manipulaci, narušení oligopolu ve finančním systému, nahrazení prostředníka technologií, podmíněnost transakcí přes smart kontrakty a automatizace

Oponenti

- rizika skrze spekulaci, volatilitu, podvody, praní špinavých peněz, přehnaná očekávání, cena vs. hodnota, problematická regulace

MUNI
LAW

Blockchain

Obsah

Dvojí chápání pojmu blockchain

Veřejný blockchain vs Privátní blockchain

Představení původní myšlenky

- Základní prvky a komponenty
- Transakce a její validace
- Asymetrické šifrování
- Tvorba nového bloku: hashovací funkce
- Validace bloků a jejich řetězení
- Motivace pro tvorbu bloků
- Důvěryhodnost záznamů a alternativní řetězce
- Změna pravidel blockchain

Variabilita podob blockchain

- Tvorba nového bloku: alternativní postupy
- Veřejné blockchainy
- Limity a nedostatky veřejného blockchain
- Správa veřejného blockchain
  - Nástroj pro legitimitu v kyberprostoru?
  - Limity důvěry skrze technologii
- Privátní blockchainy

Širší uplatnění blockchain a pilotní projekty

- Očekávání a konsorcia
- Uplatnění v rámci fintech
- Další zvažované roviny uplatnění

Dvojí chápání pojmu blockchain

Konceptuální

- myšlenkový konstrukt k řešení zajištění důvěry skrze technologii namísto instituce
- původní ideologická motivace za prvotní formulací
    - 2008 článek Satoshi Nakamoto
- *selling point* pro veřejný blockchain – podklad pro kryptoměnu Bitcoin
    - 2016 Tapscott/Tapscott – Blockchain revolution

Technologické

- řešení zabezpečení a důvěryhodnosti záznamů za kombinovaného využití asymetrického šifrování, distribuované správy záznamů, hashových funkcí a validace napříč sítí
- široké pole pro praktickou aplikaci napříč sektory
- modifikace původní technologie + opuštění ideologické motivace
- většinou zachována centrální role administrátora – privátní blockchain

Veřejný blockchain vs Privátní blockchain

Společné znaky

- šifrované zachovávání kompletní historie záznamů = zpět dohledatelná každá transakce
- diverzifikované uchovávání záznamů = potřeba neustále komunikace napříč sítí pro zachování aktuality záznamů a validity většiny uzlů

Odlišující znaky

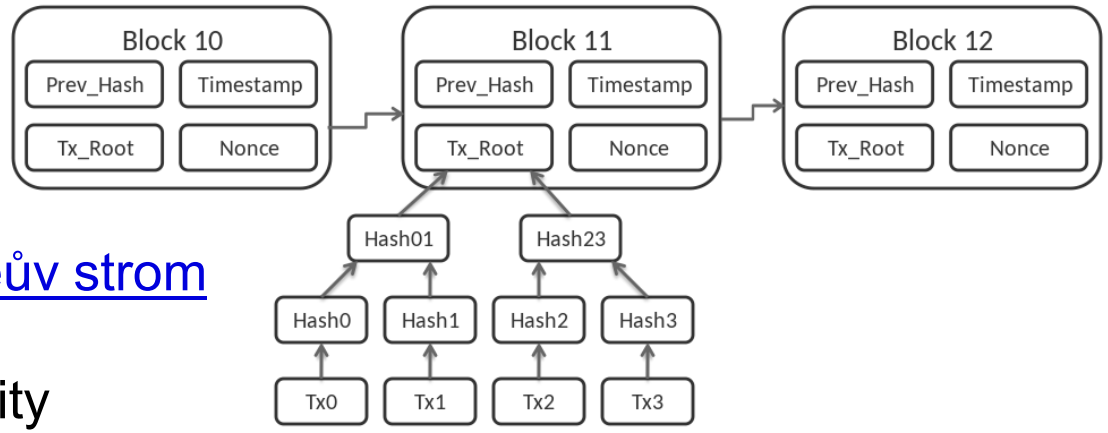
- **Veřejný blockchain** („platforma pro produkt či službu“)
  - transparentní, volně přístupný, rovnocenné postavení uživatelů ve stejné roli, decentralizovaná správa skrze konsensus / odštěpení
  - ústřední role pravidel pro tvorbu nového bloku
  - zpětný zásah do záznamů či oprava fakticky vyloučena

- **Privátní blockchain** („platforma pro interní operace či kooperaci“)
  - uzavřená síť pro určitý subjekt / skupinu subjektů, specifický účel = jedinečná architektura
  - zachována role administrátora = lze opravovat záznamy i zpětně

Představení původní myšlenky

Základní prvky a komponenty

- **Transakce**
  - datové záznamy
  - (hodnota + čas + původce + další)
- **Validace transakcí**
  - asymetrické šifrování za využití soukromého a veřejného klíče + Merkleův strom
- **Tvorba nového bloku = těžba (*mining*)**
  - pravidla pro stanovení příjemce priority pro tvorbu nového bloku
  - **Příklad Bitcoin**: Vyhledávání hashové funkce s určitými parametry
- **Blok**
  - standardizovaný šifrovaný soubor validovaných transakcí připojitelný k předchozím
- **Validace bloku**
- **Řetězení bloků (*blockchain*)**



Zdroj: Wikipedia

Transakce a její validace

- datový záznam o vzniku / změně / zániku určité informační hodnoty
- digitální zachycení libovolného obsahu
    - finanční transakce / přidělení identity / vyjádření grafické podoby / záznam události …

- **Příklad Bitcoin**:
    - platba za zboží pomocí Bitcoin skrze softwarovou peněženku uživatele
    - komunikace transakce síti => potřeba validace její přípustnosti
- **Příklad Bitcoin**:
    - peněženka si v síti potvrzuje, že uživatel má dostatek Bitcoinu pro danou transakci

Asymetrické šifrování

- Kryptografické zajištění bezpečnosti
- Asymetrické metody = pro šifrování a odšifrování potřebné odlišné klíče
- Standardní využití = elektronický podpis => přeneseno do blockchainu
- způsob potvrzení původce záznamu a jeho následná validace
- založeno na jednocestných funkcích (násobení vs. faktorizace – metoda RSA)

- **Privátní klíč**
  - přístupný pouze původci záznamu = slouží k podpisu záznamu
- **Veřejný klíč**
  - původce jej volně distribuuje se záznamem = slouží k validaci podpisu
- **Časová známka**
- **Certifikační autorita**

Tvorba nového bloku: hashovací funkce

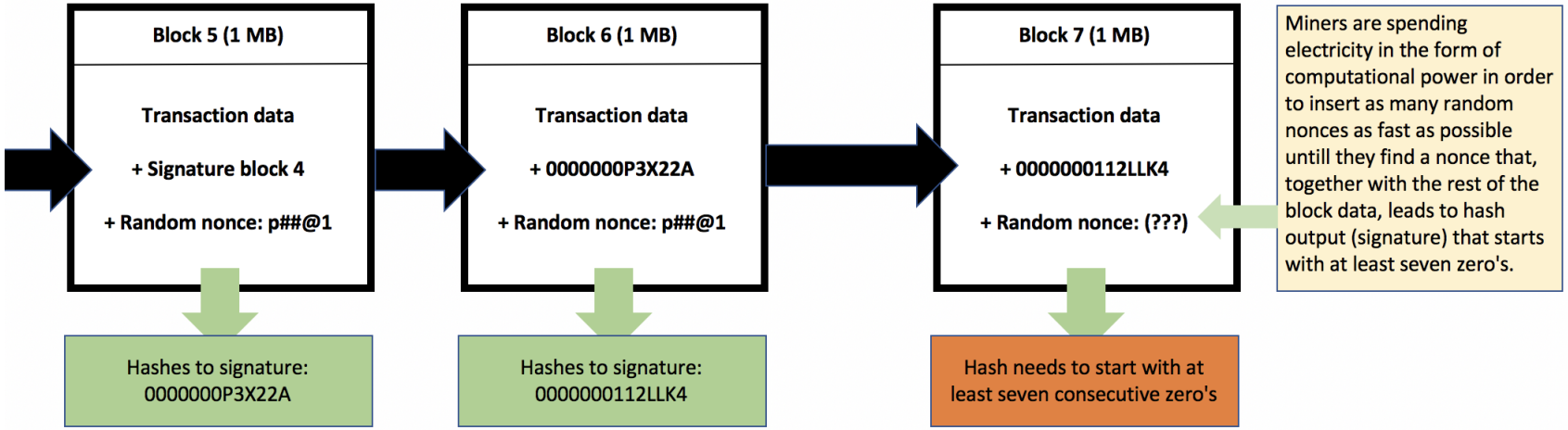
- Tradiční přístup k (náhodné) volbě priority
- Oprávnění zdůvodněno vynaloženým úsilím (proof of work)

- **Příklad Bitcoin**: nalezení čísla, které při doplnění na konec bloku a zašifrování za pomoci SHA-256 bude začínat stanoveným počtem bitů s hodnotou 0
  - hashová funkce nepodléhá předvídatelným matematickým pravidlům = číslo lze nalézt pouze za pomoci vysokého množství kalkulací, které náhodně doplňují různé hodnoty
  - *nonce* = soubor znaků doplněný do bloku, který umožní splnění pravidla
  - kontrolovaný výpočet konkrétní hash je extrémně nesnadný
- **Výhoda**
  - vysoká jistota náhodné distribuce = významné omezení koncentrace role = „zajištění důvěry skrze technologii“
- **Nevýhoda**
  - extrémní energetická náročnost – současná spotřeba cca. na úrovni Rakouska

Validace bloků a jejich řetězení

- Otázka důvěry
  - důvěra v záznam a jeho původce – elektronický podpis
  - důvěra v soubor záznamů v rámci vytvořeného bloku – hash
  - důvěra v historii transakcí - řetězec bloků propojený hashovými záznamy

- Blok = (záznamy transakcí + **hash předchozího bloku)** + nonce => **hash bloku**



Zdroj: GoodAudience

Motivace pro tvorbu bloků

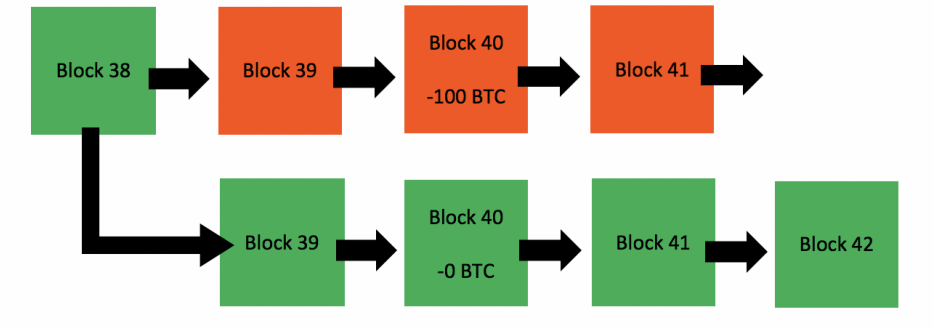
- Hledání hashů = těžba – náhodný proces + energeticky náročný
- potřeba motivace těžařů
    - poplatek za začlenění transakce / část vytvořené hodnoty bloku
- **Soutěž těžařů**

- vyšší výpočetní výkon + specializované zařízení = vyšší šance na prioritu vytvoření bloku a odměnu
- proces opakující se po každém vytvoření bloku
    - vytvoření – validace bloku – revize souboru transakcí – naplnění nového bloku a snaha o jeho prioritní tvorbu
- **Investice do těžby** závislé na vytvářené hodnotě / poptávce po validaci transakcí
- Rozsáhlé specializované prostory – Čína / významní hráči i v ČR
- Vedlejší efekty
    - nárůst v poptávce po specializovaných GPU = výrazný vliv na hlavního výrobce – Nvidia
    - nedávno byla představena Nvidia CMP pro profesionální těžbu
    - omezený rozsah bloku vs nárůst transakcí = výrazný vliv na poplatky za transakci

Důvěryhodnost záznamů a alternativní řetězce

- **Tvorba bloku náhodná** – motivace pro efektivitu procesu je čistě ekonomický zájem těžařů na výnosnosti procesu
- Blockchain nebrání vytváření alternativních řetězců (2., 3. varianty daného bloku) X validuje řetězec na bázi priority a délky řetězce

- **úspěšný těžař** = distribuce bloku sítí = validace bloku jako součást blockchain = zahájení nové soutěže o další blok
  - každý další navazující blok posiluje důvěryhodnost záznamu v tomto bloku (*confirmation*)
- **neúspěšný těžař** může vytvářet alternativní řetězec, ten však vzniká pomaleji (menší celkový výpočetní výkon) = není akceptován jako prioritní sítí = těžař není odměněn = není motivován
  - **scénář stínové těžby / dvojitá útraty (double spend) / 51% útoku**
  - důvěryhodnost záznamu X správa blockchainu a pravidla jeho fungování



Zdroj: GoodAudience

Změna pravidel blockchain

- Pravidla mechanismu konkrétního blockchainu jsou zabudována do jeho zdrojového kódu a matematické logiky, neplatí však, že jsou neměnná
- Změna pravidel možná při vytváření nových bloků
- předpoklad změny = blok s novými pravidly pro budoucí jednání převezme většina uživatelů = validace sítí + adopce těžaři

Varianty změny

- **Modifikace bez kolize s předchozími pravidly (*soft fork*)**
  - např. přidání nových forem transakcí či dodatečných prvků a funkcí
  - pouze dočasně zdvojí aktuálně přípustné bloky, které se časem sjednotí
- **Modifikace kolidující s dosavadním mechanismem (*hard fork*)**
  - rozvětvení na dva samostatné blockchainy, které dále fungují paralelně podle odlišných pravidel
  - legitimními zůstávají oba za předpokladu, že je uživatelé neopustí
  - **Příklad Bitcoin:**
    - Bitcoin Cash: blok 478558, 1.8.2017
    - Bitcoin Gold: blok 491407, 24.10.2017
    - Bitcoin SV: blok 556766, 15.11.2018

Variabilita podob blockchain

Tvorba nového bloku: alternativní postupy

Priorita na základě účasti (*proof of stake*)

- přiřazení priority na základě náhodné volby, případně náhodně za využití preferenčních faktorů, ve snaze o dosažení co nejširší distribuce oprávnění

Výhody:

- určitá kontrola nad distribucí oprávnění
- nízká energetická náročnost + přístupnost funkce všem účastníkům blockchain

Nevýhody:

- nízké náklady spojené s alternativními řetězci => problém krátkodobé důvěryhodnosti záznamů a legitimity blockchain

Různé modifikace či doplnění principu

- částečná kontrola vývojáři blockchainu – Příklad: Peercoin
- nastavením limitů
- kombinace s jiným principem
    - částečné zapojení *proof of work* (např. koncept *proof of activity*)
    - pravidla vyžadující vynaložení místa na disku (*proof of space* či *proof of capacity*)
    - vzdání se části hodnoty vytvářené v rámci blockchainu (*proof of burn*)

Veřejné blockchainy

- původní rámec, ve kterém byl blockchain nasazován (kryptoměna Bitcoin)
- **koncepční podklad pro fungování kryptoměn**
  - ideově zabarvený mechanismus = „důvěra skrze technologii nikoliv instituce“
  - vyžaduje **participativní rozhodování většiny** skrze jednání
  - uživatelé uchovávají a aktualizují lokální kopie celého blockchainu = decentralizace
  - síť uživatelů / těžařů validuje přípustnost transakce / bloku v rámci pravidel blockchainu
  - dlouhodobá změna pravidel či minulého záznamu vyžaduje spolupráci většiny
- Základní role
  - **Tvůrce**
    - stanoví výchozí pravidla fungování X nemá administrativní roli
  - **Těžař**
    - zajišťuje realizaci soutěže o tvorbu bloků = distribuci kapacit generujících záznamy – rozhoduje o konkrétním složení bloku X nemá jistotu jeho většinového přijetí + má primárně ekonomickou motivaci
  - **Uživatel**
    - vytváří záznamy a transakce, validuje je pomocí elektronického podpisu/peněženky, validuje složení bloků skrze aktualizaci své kopie blockchainu

Limity a nedostatky veřejného blockchain

Limit nárůstu objemu

- asymetrické šifrování + soutěž o prioritní bloky + velikost bloků = limit množství záznamů / transakcí

Efektivita mechanismu

- energetická náročnost soutěže těžařů + náročnost na úložný prostor a síťovo kapacitu každého uživatele

Faktická nezměnitelnost minulých záznamů

- chybná transakce / ztráta přístupu = nemožnost náhrady či opravy
- související problematika kybernetické bezpečnosti a ochrany účtů a přístupových klíčů
- **Příklad Bitcoin**: významná část v minulosti vytěžených Bitcoinů takto ztracena

Rigidita systému = změna skrze hard folk neefektivní a nejistá

Omezený reálný přínos

- robustní vnitřní mechanismus X slabá místa v napojení na vnější systémy + rigidita zvyšuje újmů v případě incidentu
- peněženky uživatelů / motivace těžařů / fungování a zabezpečení směnných bodů / absence regulace

Technické řešení jedné roviny důvěry X omezená aplikace na zbývající

- **Příklad:** Blockchain aplikace pro sdílení hudby vs. zásah od autorskoprávní ochrany

Správa veřejného blockchain
Nástroj pro legitimitu v kyberprostoru?

- koncepční podklad důvěry v regulatorní systém jako takový = společenská smlouva
  - Thomas Hobbes – Leviathan
  - John Locke – Druhé pojednání o vládě
  - Jean Jacques Russeau – O společenské smlouvě
  - John Rawls – Theory of Justice
  - **Robert Nozick – Anarchy, State and Utopia**

- **Vymahatelnost práva na internetu**
  - rychlost / absence teritoriality / závislost vnitřní logiky na lidské úvaze
  - **Lawrence Lessig – Code and Other Laws of Cyberspace + Code: Version 2.0**

- **definiční autority – regulatorní role faktická + přenesená právní**
  - ICANN, poskytovatelé služeb informační společnosti

- vymahatelnost práva X **přenesená autorita = otázka legimity**

Správa veřejného blockchain
Limity důvěry skrze technologii

- správa (*governance*) veřejného blockchain
- koncepční alternativa k institucionálním definičním autoritám
- **technologická realizace společenské smlouvy – báze jednání = konsensus účastníků**
- transparentní + pevná pravidla (X hard fork) + mechanismus tvorby důvěry (PoW/PoS)
- **paradox decentralizované správy blockchain**
- v závislosti na mechanismu různá náročnost zajištění důvěry (PoW vs. PoS)
  - energetická zátěž vs. snížená důvěra ve vzniklé bloky (riziko alternativních řetězců)
  - podmínka rentability těžby vs. riziko preferenčního postavení
- **Vili Lehdonvirta – The Blockchain Paradox**
  - blockchain řeší důvěru ve vnitřní správě X nebrání zneužití na úrovni nastavení definičních norem sítě
  - kontrola nad pravidly legitimizována právem silnějšího/výkonnějšího = absence struktury a odpovědnosti - pouze zástěrka aktivní participace většiny?

Privátní blockchainy

- Snaha o využití technologických benefitů mechanismu při konkrétní aplikaci
- Zachování existujícího rámce institucionálního zajištění důvěry + jeho posílení skrze technologickou platformu
- přístup k posílení stávajících šifrovaných, decentralizovaných databází či jejich nové zavedení do interních či kooperativních procesů

Charakteristika

- **Role administrátora**
  - možnost měnit pravidla i záznamy, či jinak spravovat blockchain
- **Absence soutěže těžařů**
  - optimalizace nákladů, upravená distribuční pravidla
- **Omezená oprávnění k tvorbě záznamu**
  - kooperující subjekty / vnitřní složky subjektu
- **Různé úrovně oprávnění**
  - např. právo vytvářen záznam vs. pouze čtení záznamů

Širší uplatnění blockchain a pilotní projekty

Očekávání a konsorcia

- **Fintech** – značná očekávání ohledně dopadu a přínosu technologie
  - analýza Mezinárodního měnového fondu
  - analýza ESMA
  - analýza US Federal Reserve
  - zpráva World Economic Forum – většina bank zkouší integraci technologie

- **Kooperační iniciativy**
  - Hyperledger project (Linux Foundation) – open source blockchain platforma
  - Corda (R3) – podnikatelská blockchainová platforma rozsáhlého konsorcia
  - Global Blockchain Business Council

Uplatnění v rámci fintech

mezinárodní platební síť
- **Příklad:** Visa B2B Connect

pojišťovací databáze
- **Příklad:** pilotní projekt Allianz

platforma pro sdílení informací a metadat transakcí
- **Příklad**: NASDAQ Linq

obchodní platforma
- **Příklad:** projekt konsorcia Commonwealth Bank

zúčtovací a clearingová platforma
- **Příklad:** start-up Axoni

Další zvažované roviny uplatnění

Pozemkové registry
- **Příklad:** Švédsko

Důvěra v záznamy

Obchodní rejstříky
- **Příklad:** Dubaj
- **Příklad:** Estonsko

Dodavatelský řetězec
- **Příklad:** Target

Elektronické nákladní listy a údaje o zboží
- **Příklad:** IBM/Maersk

Validace pohybu uměleckých děl

Přehled dalších nasazení DLT technologie ze strany významných korporací

MUNI
LAW

Kryptoměny

Obsah

Hotovost vs. Kreditní karta vs. Kryptoměna

Specifika transakcí v digitálním prostředí

Kryptoměna

Bitcoin

Prostředí kryptoměn

- Peněženky (cryptocurrency wallets)
- Směnárny kryptoměn
- Utváření hodnoty kryptoměny
- Initial Coin Offering (veřejná nabídka kryptoměny)
- Rizika spojená s kryptoměnami
- Incident směnárny Mt. Gox
- Podvody s kryptoměnami

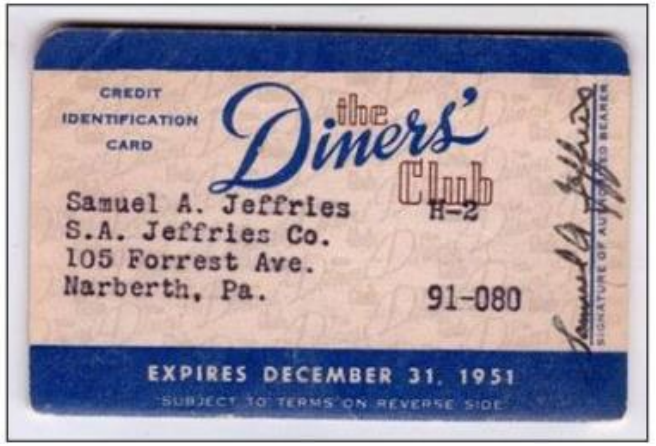
Alternativní kryptoměny

Hotovost vs. Kreditní karta vs. Kryptoměna

Hotovost

- Přednosti
  - nevysledovatelná a anonymní
  - volné užití a okamžité transakce

- Překážky
  - fyzická podoba a limitovaná dělitelnost



- Postupná virtualizace transakcí
- únor 1950 – první kreditní karta - pro platby v restauracích
- bezhotovostní transakce => virtualizace finančního sektoru => rozvoj burzovních nástrojů a instrumentů
  - dnešní pseudo-hotovostní svět (nostalgická jistota hotovosti X praktická digitalizace transakcí)
- Svatý grál fintech = Digitální hotovost
- hotovost funkční v digitálním prostředí – kryptoměna?

Specifika transakcí v digitálním prostředí

- síť Internet = původ – 60.léta – ARPANET (grant DARPA)
- založeno na premise, že všichni uživatelé jsou důvěryhodní (výzkumníci…)
- zachováno v základních protokolech = přetrvávající problém v konfliktu s realitou
- BFT (*Byzantine fault tolerance*)
- „problém dvou armád“ (*Byzantine generals problem*)
- potřeba shody X absence důvěryhodnosti => potřeba centrální autority
- X snahy o hledání alternativy => decentralizované sítě
    - koncepční báze Bitcoin = podmínka pro využití jako digitální hotovost

Kryptoměna

- digitální/virtuální aktivum založené na kryptografickém schématu zajištění bezpečnosti
- zpravidla decentralizované systémy založené na veřejném blockchainu
- **"důvěra založená na technologii"**
- absence zjevné centrální definiční autority
- "alternativa" k institucionálním aktivům vydávaných v rámci národních systémů a režimů
- první a nejvýznamnější příklad: Bitcoin
- dnes tisíce alterantivních kryptoaktiv (*altcoin*)
- transakce s tokeny
- token = zástupný záznam v databázi (např. tokenizace v bankovních operacích)

Bitcoin

Počátek

- experiment v digitální neregulované měně
- vhodné načasování – 2009 – finanční krize (*credit crunch*)
- popularizace vzdoru vůči institucím (vlády/banky) = podpora alternativních řešení
- rozmach dark webu
- online tržiště s drogami - **Příklad**: Silk Road
- nové modely pro trestnou činnost
- digitální dealer - **Příklad**: Dropgangs
- ransomware
- podvody s obchodováním s kryptoměnami
- praní špinavých peněz
- synergický efekt s rozvojem role influencerů a online komunit
- YouTubeři („podomní prodejci virtuálního věku“)
    - **Příklad:** HODL (*hold on for dear life*)
- celebrity – volatilita = „loterie“ = propagace skrze „výherce“
    - **Příklad**: Tyler and Cameron Winklevoss
    - kryptoměny jako „náboženství“ = noví proroci a misionáři

Historie vývoje ceny a objemů

první kryptoměna postavená na úvodní koncepci veřejného blockchainu
fungování zahájeno v roce 2009, významná fluktuace zájmu, minulý vrchol přelom 2017/2018, nový průlom počátek 2021

Relativní parametry

- počet Bitcoinů
  - každý blok = 12,5 bitcoinu
  - nyní cca. 18,6 milionů
  - celkový počet (v roce 2140) = 21 milionů (= technologicky programovaná vzácnost)
- Bitcoin blockchain
  - velikost = nyní cca. 317 GB
  - délka – cca. 671 500 bloků
- Bitcoin blok
  - velikost = cca 1MB
  - frekvence = cca 144 bloků za den (= 900 nových Bitcoinů, protože 6,25 Bitcoinů na blok)
- Bitcoin transakce
  - 4,6 transakcí/sec X VISA - 1700 transakcí / sec
- Bitcoin negativní dopady
  - roční energetická náročnost – cca. 78 TWh (= cca. Rakousko)
  - dopad na životní prostředí – v roce 2018 každý 1 USD vytvořené hodnoty Bitcoin vedlo k 0,49 USD škodám na zdraví a živ. prostředí – hlavní zdroj energie = uhelné elektrárny

Prostředí kryptoměn

Peněženky (*cryptocurrency wallets*)

- široké spektrum dostupných softwarových řešení účtů

A) nehostované softwarové peněženky, kde má uživatel kontrolu nad soukromým klíčem
- např. Bitpay wallet

B) hostované softwarové peněženky, kde uživatel nemá kontrolu nad soukromým klíčem
- např. Coinbase wallet

C) hardwarová peněženka, ve které je zachycen soukromý klíč
- např. Trezor wallet

D) papírová peněženka
- online generátor soukromého klíče pro transakci a adresy účtu pro vytištění

Směnárny kryptoměn

- Nezbytný mezičlánek pro uživatele kryptoměn pro nabytí těchto aktiv
- vedle odměny za těžbu či jiný specifický participační mechanismus daného tokenu
- Srovnatelné fungování s běžnými směnárnami
- **Směna tradičních směn za kryptoměny** (např. USD za Bitcoin a zpět)
- **Směna kryptoměn mezi sebou**
- Omezená regulace + mezinárodní dosah = „divoký západ“ digitálního věku
- Stovky směnáren, různá reputace, řada incidentů a podvodů
- Nejvýznamnější podle objemu
- Binance / HTBC / Hydax Exchange / Dsdaq / CITEX
- alternativa – Atomic swaps = přímé peer-to-peer směny kryptoměn mezi uživateli bez centralizované směnárny – vč, off-chain swapu (tzn. mezi měnami), zpravidla koordinováno decentralizovanou směnárnou – např. Komodo

Utváření hodnoty kryptoměny

1) Ideologická

- dlouhodobí držitelé - založena na víře v budoucí systémovou důležitost kryptoměny

2) Praktická

- použitelnost tokenů jako alterantivní platidlo, jako „dýško“ v online komunitách, či jako podklad služeb
- nedávný vývoj – vstup společností Tesla , Mastercard a BlackRock
- použitelnost kryptoměny jako „digitální hotovost“ vs. extrémní volatilita a iracionální vývoj hodnoty

3) Spekulační

- krátkodobá riziková investice do kryptoměny v reakci na její rostoucí popularitu a předpoklad skokového či dalšího růstu ceny
- fenomén FOMO (*fear of missing out*) – velmi silný u kryptoměn, zvláště u Bitcoin na začátku 2021

4) Kriminální

- využití anonymity či jiné vlastnosti kryptoměny pro obchod s nelegálními produkty, financování trestné činnosti, praní špinavých peněz či vydírání obětí počítačové kriminality (ransomware)

5) Geopolitický nástroj?

- proti sankcím a dolarové hegemonii / pro financování hybridní války

Initial Coin Offering
(veřejná nabídka kryptoměny)

- možnost financování podnikatelského záměru
- alternativa k odvážným investorům, dluhopisům či úvěrům
- paralela ke sbírce / crowdfundingové akci – „crowdsales“
- kryptoměna = token s právy a nároky investorů
- populární mezi start-upy - minimální regulace, minimální byrokracie
- kontroverzní z hlediska pravidel finančního trhu (neregulováno / zakázáno)
- časté případy podvodů na nedostatečně informovaných investorech
- prospekt => shromažďování investic => splnění parametrů X vrácení investic

Initial Coin Offering
(veřejná nabídka kryptoměny)

- podobnost s veřejnou nabídkou akcií (IPO)
- nástroj pro financování start-upů
- odlišnosti od IPO
    - investoři X podporovatelé (supporters)
    - decentralizovaný proces (= mimo burzu)
    - neregulované/podregulované (= „investiční divoký západ“)
    - bez institucionálního dozoru
    - výrazně flexibilnější ohledně formátu, podmínek, požadavků, informací
- úspěšné příklady
    - Ethereum – 2014 – pionýrské ICO
    - Antshares(=NEO) – 2015 – růst ceny z 0,03 $ na 50 $ = extrémní ROI
    - filecoin – 2017 – shromážděný objem investic 257 milionů $
- studie předpokladů pro úspěšné ICO

Rizika spojená s kryptoměnami: Spekulace

- Popularizované investiční aktivum
- potenciál vysoké výnosnosti a likvidity
- V zásadě neregulované prostředí - relevantní rizika
- velmi vysoká investiční rizikovost, netradiční vývoj a utváření hodnoty = nepředvídatelnost
- vysoká intenzita podvodů v rámci ICO / sněmáren / transakcí
    - **Příklad:** podvody s množstvím transakcí na směnárnách (až 95 % uměle provedených transakcí)
    - Podvody a Insider trading - propagace tokenu influencerem a následný hromadný výprodej
    - Podvody v rámci atomic swaps
- boom kybernetických útoků a krádeží soukromých klíčů / tokenů + ransomware
- bubliny a posilování tržních výkyvů skrze strojové obchodování a smart kontrakty – lavinové prodeje
- úzká vazba na nelegální aktivity – zajištění anonymity / pseudonymity
- rostoucí pozornost regulátorů = vliv na volatilitu a nárůst pochybností o ospravedlnění současné hodnoty
- vysoká citlivost na široké spektrum zpráv a tržních podnětů = extrémní volatilita

Rizika spojená s kryptoměnami: Další

- Rostoucí hodnota kryptoměnových aktiv = větší obava uživatelů o bezpečnost jejich investice = popularizace služeb správců
    - odpoutání se od konceptu blockchain – závislost na jednom slabém článku = instituce správce (platforma peněženky / směnárna / správce hesel / broker apd.)
    - absence regulatorního dozoru = přítomnost různě důvěryhodných a fungujících subjektů
    - Hlavní riziko = podvody a počítačové tresné činy (hacking) ve vztahu k těmto prostředníkům
- Časté rozsáhlé krádeže schraňovaných kryptoměn velkými směnárnami
- **Příklady** s hodnotami ztracených kryptoměn v době incidentu
    - Coincheck – cca 530 mil. USD
    - Mt. Gox – cca. 473 mil. USD
    - Bitfinex – cca. 72 mil. USD
- Další rizika
    - zapomenutá hesla – nemožnost obnovení / náhrady
    - ztracené disky – ztráta hardwarové peněženky / správce hesel
    - zkrachovalé burzy – absence pojištění investice či jiné formy záchranné sítě

Incident směnárny Mt. Gox

- svého času největší směnárna kryptoměn (2014 – 70 % Bitcoinových transakcí)
- incident z roku 2011
- podvodné narušení zabezpečení směnárny a následné krátkodobé umělé snížení ceny obchodovaných Bitcoinů na zlomek
- bankrot 2014 po oznámení, že směnárna nemá kontrolu nad 850 000 Bitcoiny (cca. 1/12 všech Bitcoinů v té době, hodnota cca. 480 milionů USD)
- incident způsobil dočasný celosvětový pokles ceny Bitcoinu o 36 %
- ve chvíli incidentu nebyl jasný důvod ztráty daných tokenů
- vyšetřování 2015 – postupné vykrádání operativní peněženky směnárny v období od 2011 do 2014
- případ je stále vyšetřován + konkursní řízení stále běží

Podvody s kryptoměnami

- většina ztrát kryptoměn spojena s podvody spíše než hackingem – v roce 2020 celkem kryptoměny v hodnotě cca. 1,9 mld. USD
- v rekordním roce 2019 takto ztraceny kryptoměny v hodnotě 4,5 mld. USD – report
- **Příklady:**
  - 2020 KuCoin krádež v hodnotě cca. 150 mil. USD - report
  - 2019 krádež ze směnárny BITpoint – cca. 28 milionů USD
  - 2019 hack směnárny Binance – cca. 7000 Bitcoinů a přihlašovací údaje – hodnota cca. 40 mil. USD – report
  - phishingový útok trvající přes 3 roky, údajně se škodou až 100 milionů USD - report
  - typosquatting útok (např. kreken.com namísto kraken.com) – 4000 obětí, cca. 27 milionů USD - report
  - OneCoin – vyšetřováno jako zjevné Ponziho schéma od roku 2017 – report
  - 2018 – italská směnárna BitGrail okradena o RXP v hodnotě cca. 170 milionů USD - report

Alternativní kryptoměny

Nejvýznamnější altcoiny

- snaha o napodobení úspěšného obchodního modelu Bitcoin
- snaha o vyšší flexibilitu / širší uplatnění / vyšší mírou soukromí a anonymity / vyšší frekvenci transakcí / nižší energetickou náročnost / alternativní postupy tvorby důvěry atd.
- Ethereum / XRP / Litecoin / EOS / Stellar / Cardano / Monero / TRON / Zcash / Dogecoin
- projekt FB Libra => 2019 Diem

Ethereum

- https://www.ethereum.org/
- open source varianta kryptoměny druhé generace
- spuštěna v červnu 2015, tvůrci Vitalik Buterin, Gavin Wood
- druhá nejhodnotnější a nejrozsáhlejší síť kryptoměny
- vysoká variabilita odvozených aplikací
- Případ DAO (decentralized autonomous organization) - 2016
    - nadstavba nad Ethereum – cca. 14 % tokenů X chyba = hack a hard fork
    - „starý“ blockchain = Ethereum Classic (ETC) X nový blockchain Ethereum (ETH)
- Ethereum Virtual Machine – nástroj pro realizaci smart kontraktů
- Enterprise Ethereum Alliance – 2017 – Fortune 500 společnosti – privátní blockchainy
- Vývoj hodnoty a objemů – boom počátkem 2021

XRP

- https://www.ripple.com/xrp/
- open source „kryptoměna“ na síti uskupení okolo společnosti Ripple
- příklad centralizovaného řešení blockchain důvěryhodnosti (Ripple drží 60% tokenů)
- jedno z využití blockchainu X další paralelní projekty, např. burza kryptoměn
- vznik 2012 – úspornější, flexibilnější a rychlejší alternativa k Bitcoinu
- jiný mechanismus – všechny tokeny vytěženy od začátku, transakce na základě konsensu sítě, poplatek = zničení části tokenů = konstatní snižování počtu tokenů v síti
- vyšší rychlost (cca 2 sec na validaci transakce vs. minuty v případě Bitcoin)
- minimální poplatky za transakci
- XRP = zúčtovací prvek sítě nikoliv „komodita“ – síť RippleNet
- prioritní projekty – mezinárodní mezibankovní transakce a převody mezi finančními institucemi
- Vývoj hodnoty a objemů – vrchol 2018, na počátku 2021 pouze malý nárůst ceny X velký nárůst objemu

Litecoin

- https://litecoin.org/cs/
- jeden z prvních altcoinů, úzké propojení s Bitcoinem
- open source kryptoměna, vznik 2011, tvůrce: Charles Lee
- plná decentralizace - algoritmus Scrypt (inovace – vliv na další generace altcoinů)
- upravený výpočet v rámci těžby = nižší náročnost na hardware – těžba za pomoci grafických karet = vyšší distribuce role těžařů v rámci sítě (i slabší zařízení)
    - X 2014 – ASIC (*application-specific integrated circuit*) Titan = změna technologických možností, znevýhodnění těžařů s grafickou kartou = ztráta „demokratické“ základny těžařů = propad zájmu a ceny
- 2017 – upgrade SegWit (vyšší kapacita, náprava chyb za hlavními incidenty) a upgrade Lighting Network - možnost decentralizované směny kryptoměn (atomic swaps) = opětovný nárůst zájmu, paralelní růst do extrému s Bitcoinem na konci 2017
- Vývoj ceny a objemů – podobně i nyní na počátku 2021 významný růst paralelně s Bitcoin

Monero

- https://www.getmonero.org/
- open source kryptoměna, těžba na bázi PoW
- hl. deviza = zvýšená anonymita uživatelů – metoda síťování Dandelion++
- zvýšená popularita u kriminálních živlů – nahradila Bitcoin na tržištích dark webu a v požadavcích v rámci ransomware (**Příklad:** WannaCry)
- 2018 – využívána pro 44 % ransomware požadavků
- vznik 2014, tvůrce Nicolas van Saberhagen
- odolné vůči ASIC - algoritmus CryptoNight
- 2019 – algoritmus RandomX
- 2020 – daňový úřad v USA (IRS) usiluje s pomocí společností INTEGRA FEC LLC and CHAINALYSIS INC. o prolomení anonymity a možnost trasování
- Vývoj ceny a objemů – jako u většiny kryptoměn došlo významnému nárůstu počátkem 2021 x nedosahuje však popularity a vrcholu z konce 2017

Zcash

- https://z.cash/
- open source kryptoměna, odvozená z Bitcoin, těžba PoW
- vznik 2013, tvůrci: Daira Hopwood, Sean Bowe, Taylor Hornby, Nathan Wilcox
- vznik skrze venture investory, nikoliv ICO
- speciální kryptografický protokol zk-SNARK
- odolná ASIC - algoritmus Equihash
- zvýšená úroveň anonymizace všech transakcí = populární pro nelegální obchody na dark webu
    - 2020 pochybnosti o úrovni anonymizace uživatelů – článek „Alt-Coin Traceability“
    - 2020 – dle Chainanalysis je naprostá většina transakcí (99%) přes Zcash dohledatelná
- Vývoj a objemy – nárůst počátkem 2021, vrchol zůstává koncem 2017

Dogecoin

- https://dogecoin.com/
- vznik prosinec 2013, tvůrci: Billy Markus, Jackson Palmer
- podklad pro vznik – nejpopulárnější meme roku 2013 se psem Shiba Inu
  - pro lepší pochopení - propagační video z 2014
  - extrémní množství tokenů – do roku 2015 naprogramováno vytěžení 100 miliard Dogecoinů
- bez praktického využití
  - ve 2014 populární na sociálních sítích jako „dýško“ pro kvalitní obsah
  - čilá online komunita, která nalézá nová promo uplatnění
    - podpora jamajských bobařů pro cestu na zimní olympijské hry 2014
    - sponzoring vozu v prestižních závodech NASCAR
- Vývoj ceny a objemů
  - zcela uměle vytvořený boom počátkem 2021 skrze tweety Elona Muska
  - „vtípek“, který dosáhl na tržní kapitalizaci přes 10 mld. USD (8.2.2021)

Kryptoměny jako symbol generace

- kryptoměny vznikly jako „hračky“ IT nadšenců bez reálného obchodního modelu a plánování
- původní koncept Bitcoin byl velice idealistický
- 2010 – rok po spuštění blockchain Bitcoin – případ „nejdražší“ pizzy v historii (10 000 BTC za 2 velké pizzy) = kryptoměna blíže penězům ze hry Monopoly než platidlu
- **synergie trendů** – finanční krize / milleniálové / rozmach sociálních sítí / kultura hipster / popularizace IT řešení a digitalizace služeb / rozmach dark webu a alternativních využití kryptoměn / spekulační boom v důsledku Covid pandemie
    - boom propagace kryptoměn jako trendy inovace + příklady úspěšných „investorů“ = run na Bitcoin
- **spekulace, iracionální tvorba hodnoty, tržní bublina**
    - symbol generace – IT vzdělanost + tlak na úspěch a zisk + hledání rychlých a snadných řešení
    - kryptoměny ideální lákadlo, výborný marketingový artikl
    - FOMO / investice nikoliv na základě racionálních úvah o hodnotě, ale na základě víry v nekonečný růst = znaky chování členů kultu = extrémně zajímavý sociologický jev
- **produkt charakterizující a limitující se na jednu generaci?**
    - nesnadné pochopení ze strany starších generací – absence nezbytné perspektivy generace online komunit X boom počátkem 2021 skrze širší povědomí a FOMO ze strany majetnějších spekulantů?

Bizarní kryptoměny

- Popularizace kryptoměn přinesla široké spektrum snah o využití trendů pro nesouvisející účely
- Za mnoho příkladů lze uvést:
- KodakCoin
  - pokus bankrotující americké společnosti zmást investory skrze trendy heslo kryptoměna
- Venezuelan Petro
  - populistická snaha diktátora Mandura odolat finančnímu tlaku mezinárodní komunity
- PotCoin
  - platforma pro legální obchod s marihuanou
- TrumpCoin
  - *„A digital cryptocurrency supporting Patriots around the world.“*
- PutinCoin
  - *„PutinCoin was created to pay tribute to the people and the president of one of the largest and greatest countries in the world: Russia!“*
- CatCoin
  - *„Catcoin is a cat version of Litecoin“*

Bizarní kryptoměny

- Další příklady, pro ilustraci mezigeneračních bariér, které okolo online komunity propagující kryptoměny stojí
- Coinye
  - neúspěšná snaha o parazitování na „image“ celebrity Kanye West z roku 2014
- BitCoen
  - kryptoměna založená na specifičnosti židovské komunity a pro její potřebu
- Useless Ethereum Token
  - přesně to, co lze vyčíst z názvu
  - *"The world's first 100% honest Ethereum ICO. You're going to give some random person on the internet money, and they're going to take it and go buy stuff with it. Probably electronics, to be honest. Maybe even a big-screen television. Seriously, don't buy these tokens."*
- **Cthulhu Offerings**
  - Podklad = hororová povídka H.P. Lovecrafta The Call of Cthulhu z roku 1928
- **Skincoin**
  - tokeny pro nákup grafických úprav vzhledu zbraní v online herních komunitách
- Finally Usable Crypto Karma
  - pro vysvětlení akronym a video
  - současná tržní kapitalizace kryptoměny = maximální tržní kapitalizace cca. 8 mil. USD (17.9.2017)

MUNI
LAW

Právní regulace kryptoaktiv

Obsah

Regulace trhů s kryptoaktivy v rámci EU

Návrh nařízení o trzích s kryptoaktivy

Právní úprava v ČR – soukromoprávní rovina

Právní úprava v ČR – veřejnoprávní rovina

Situace mimo EU

- Přístup ve Spojených státech
- Přístupy v dalších zemích

Regulace trhů s kryptoaktivy v rámci EU

- **Akční plán pro finanční technologie: Za konkurenceschopnější a inovativnější evropský finanční sektor** (EK 3/2018)
  - potenciál kryptoaktiv a technologie blockchain pro finanční trhy a infrastrukturu – proměna způsobu, jakým jsou informace nebo aktiva v digitálních sítích vyměňovány, ověřovány, sdíleny a zpřístupňovány / očekávatelná klíčovoá složka digitální ekonomiky a společnosti
  - vysoká rizikovost investic do kryptoaktiv – problematika volatility spolu s nedostatečnou transparentností a integritou trhu
- **Doporučení k ICO a kryptoaktivům** (ESMA 1/2019)
  - některá kryptoaktiva mohou být vnímána jako investice podobná CP
  - i tradiční finanční aktiva začínají být vydávána a převáděna přes DLT
  - kryptoaktiva, která naplňují podmínky k tomu, aby byla kvalifikována jako finanční instrument, by měla být regulována
- **Doporučení pro Evropskou komisi ke kryptoaktivům** (EBA 1/2020)
  - užití kryptoaktiv se vyvinulo nad rámec kryptoměn
  - rizika při nakládání s kryptoaktivy pro spotřebitele, provozní odolnost a integritu trhů

Regulace trhů s kryptoaktivy v rámci EU

- **Priority pro digitální transformaci finančního sektoru EU** (EK 9/2020)
  - Předpoklad, že digitální budoucnosti financí je a klíčové role digitálních technologií při oživování a modernizaci
  - 1. Odstranit roztříštěnost digitálního trhu finančních služeb a umožnit spotřebitelům přeshraniční přístup ke službám
  - 2. Usnadňovat digitální inovace skrze regulatorní rámec
    - Umožnění vzniku trhů EU s kryptoaktivy a tokenizovanými finančními nástroji
    - Do roku 2024 zavést komplexní regulatorní rámec pro tuto oblast
    - Potenciál pro centrální banky, které mohou vyvinout digitální měny centrálních bank
    - Podnícení rozvoje technologií distribuované účetní knihy s nízkými nebo nulovými emisemi a internetu věcí
  - 3. Vytvořit evropský prostor pro finanční data za účelem podpory inovace a zlepšení přístupu k datům a jejich sdílení
  - 4. Řešit nové výzvy a rizika spojená s digitální transformací – zajištění finanční stability, ochrany spotřebitele, integrity trhu, spravedlivé hospodářské soutěže a bezpečnosti

Regulace trhů s kryptoaktivy v rámci EU

- **směrnice (EU) 2018/843 - 5. AML směrnice** - transpozice k 1/2020 (do AML zákona 253/2008)
  - vymezení **virtuální měny** a poskytovatele virtuální peněženky
    - digitální reprezentace hodnoty, která není vydána či garantována centrální bankou ani orgánem veřejné moci, není nutně spojena se zákonně stanovenou měnou a nemá právní status měny či peněz, je však fyzickými nebo právnickými osobami přijímána jako prostředek směny a může být elektronicky převáděna, uchovávána a obchodována
  - nové povinnosti pro poskytovatele směnárenských služeb mezi virtuálními měnami a měnami s nuceným oběhem a poskytovatelé virtuálních peněženek - registrace a další povinnosti
- neměly by být zaměňovány s
  - kryptoaktivy kvalifikovatelnými jako „**finanční nástroje**“ ve smyslu směrnice (EU) 2014/65 o trzích finančních nástrojů
  - kryptoaktivy kvalifikovatelnými jako **"elektronické peníze"** ve smyslu čl. 2 bodu 2 směrnice 2009/110/ES o přístupu k činnosti institucí elektronických peněz
  - s širším pojmem „**peněžní prostředky**“ ve smyslu čl. 4 bodu 25 směrnice (EU) 2015/2366 či s peněžní hodnotou uchovávanou na nástrojích, pro něž platí výjimka podle čl. 3 písm. k) a l) této směrnice
  - s herními měnami, které lze používat výlučně v rámci konkrétního herního prostředí

Regulace trhů s kryptoaktivy v rámci EU

- **návrh nařízení o trzích s kryptoaktivy (nařízení MICA)**
- návrh nařízení o digitální provozní odolnosti finančního sektoru
  - jednotné požadavky týkající se bezpečnosti sítí a IS využívaných finančními subjekty
  - návrh zahrnuje též nové formy finančních obchodních modelů (poskytovatelé služeb spojených s kryptoaktivity, vydavatelé kryptoaktiv, vydavatelé tokenů vázaný na aktiva)
  - zásadní výzvou bude především koordinace prosazování a vymáhání příslušných regulatorních požadavků
  - reflexe již dosažené míry standardizace (ISO rodiny 27k), posun ve standardizaci předvídané aktem o kybernetické bezpečnosti (nařízení 2019/881), klíčová budoucí role technických standardů ESA
- návrh nařízení o pilotním režimu pro tržní infrastruktury na bázi DLT
  - stanovení požadavků na mnohostranné obchodní systémy a systémy vypořádání obchodů s CP, které využívají DLT

Návrh nařízení o trzích s kryptoaktivy

- cíle: právní jistota / podpora inovací / ochrana investorů a spotřebitelů / finanční stabilita

- **pojem "kryptoaktiva"** - digitální zachycení hodnoty nebo práv, které může být převáděno a ukládáno elektronicky pomocí DLT nebo pomocí podobné technologie
- **Druhy:**
  - 1) kryptoaktiva mimo působnost nařízení (**finanční nástroje / elektronické peníze** / vklady / strukturované vklady / sekuritizace)
  - 2) **"token vázaný na aktiva"** (stablecoins) - jeho cílem je udržet stabilní hodnotu navázáním na hodnotu několika fiat měn, které jsou zákonným platidlem, jedné nebo několika komodit nebo jednoho či několika kryptoaktiv, případně na hodnotu kombinace těchto aktiv
  - 3) **"elektronický peněžní token"** (některé kryptoměny) - hlavním účelem je použití jako prostředku směny a jeho cílem je udržet stabilní hodnotu navázáním na hodnotu fiat měny, která je zákonným platidlem
  - 4) „kryptoaktiva jiná než tokeny vázané na aktiva nebo elektronické peněžní tokeny“ (např. **utility tokeny** = určen k poskytování digitálního přístupu ke zboží nebo službě a přijímán pouze vydavatelem tokenu).

- vydavatel kryptoaktiv / veřejná nabídka / služby související s kryptoaktivy (úschova a správa / provoz obchodní platformy / směna kryptoaktiv za fiat měnu/jiná kryptoaktiva / provádění příkazů v zastoupení třetích stran / uvádění kryptoaktiv / přijímání a předávání příkazů / poskytování poradenství)
- povolení / bílá kniha / povinnosti vydavatelů / propagační sdělení / informování držitelů / střet zájmů / kapitálové požadavky / rezerva aktiv / významné tokeny a dodatečné povinnosti

Právní úprava v ČR – soukromoprávní rovina

- **nutno odlišovat právní rámec uvnitř systému kryptoaktiva a vně**
  - množina a různorodost kryptoaktiv = nemožnost jednotného závěru či popisu pravidel
- **práva uvnitř systému kryptoaktiva (relativní povahy)**
  - řešena primárně vlastním systémem kryptoaktiva = na bázi parametrů daného blockchain/DLT
  - soukromé blockchainy / uzavřené systémy => smluvní báze vztahů uvnitř systému kryptoaktiva => stanovení jurisdikce i rozhodného práva (=> nařízení Řím I)
  - veřejné blokchainy - **Příklad Bitcoin:** princip konsensu mezi nody (= zařízeními s celou historií blockchain) - změny = soft fork/hard fork => smluvní povaha vztahu pro určení rozhodného práva (analogie SDEU Martin Peters) X problematická klasifikace => nepravděpodobná vazba mezinárodních kryptoaktiv na české závazkové právo

Právní úprava v ČR – soukromoprávní rovina

- **práva vně systému kryptaktiva (absolutní povahy)**
  - klasifikace a uplatnění pr. nároků provázáno s klasifikací právních vztahů uvnitř
  - **nehmotné aktivum** - vazba na movitou věc není nezbytná (soukromý klíč k Bitcoin účtu = informace = může být v zařízení X v paměti / blockchain = záznam transakcí bez vlastní hodnoty - nezbytný konsensus a shoda s distribuovanými kopiemi)
  - X práva duševního vlastnictví / chráněné informace (osobní údaje / obchodní tajemství)
  - sekundární povaha věcněprávní klasifikace kryptoaktiva = primární nosič je věc, provázanost s ním = provázanost právního nároku
  - **nutno odlišovat dílčí projevy věcněprávního nároku** => složitost otázky určení rozhodného práva pro pr. nárok k aktivu
    - analogická aplikace čl. 14 Řím I = postoupení pohledávky? => rozdílnost národních úprav - návrh nařízení o právu rozhodném pro účinky postoupení pohledávek na třetí strany)
    - očekávání spojená s technickými vlastnostmi systému = analogie podnikové prestiže (*goodwill*)? => právo místa sídla / bydliště? X nejasná a nepraktická aplikace
- **věcněprávní povaha kryptoaktiva dle OZ**
  - § 489 OZ - odlišnost od osoby / sloužit potřebě lidí / ovladatelnost => nehmotná movitá věc
  - ČNB - kryptoměny nevykazují znaky investičních nástrojů (CP/ZCP/derivátu) X teoretické naplnění znaků ZCP stran specifického kryptoaktiva X nemá zřejmý benefit

Právní úprava v ČR – veřejnoprávní rovina

- **rozšířená transpozice 5. AML směrnice do AML zákona 253/2008**
  - povinné osoby v § 2 poskytující služby spojené s virtuálním aktivem (§ 4 odst. 8)
  - **virtuální aktivum** (§ 4 odst. 9)
    - složitá definice s řadou výjimek (nejedná se o CP, investiční nástroj, peněžní prostředek podle zákona o platebním styku atd.)
    - elektronicky uchovatelná nebo převoditelná jednotka, která je a) způsobilá plnit platební, směnnou nebo investiční funkci, bez ohledu na to, zda má nebo nemá emitenta a je b) jednotkou podle § 3 odst. 3 písm. c) bodů 4 až 7 zákona o platebním styku (platební prostředek pouze pro úzce vymezený okruh užití)
- **spekulace** = správa vlastního majektu X cizí majetek – živnostenské oprávnění / X těžba – živnostenské oprávnění
- **Zisky podléhají dani z příjmu** (není výslovně upraveno = nutno vycházet z obecných principů a pravidel)
  - příjem ze samostatné činnosti dle § 7 zákona o dani z příjmu, resp. ostatní příjem dle § 10 zákona o dani z příjmu
    - obtížná spravovatelnost příjmů dosažených směnou jedné kryptoměny za jinou ze strany správce daně, nemožnost osvobození, nejasnost týkající se zařazení příjmů při využívání kryptoměn jako investičního aktiva, složitý způsob stanovení základu daně z ostatních příjmů
  - peněžní (převod kryptoměny na běžnou měnu) i nepeněžní příjem (převod mezi kryptoměnami) / platí i pro těžbu
- **Směna zřejmě nepodléhá dani z přidané hodnoty**
  - rozsudek SDEU z roku 2015 ve věci C-264/14, Hedquist

Situace mimo EU

Přístup ve Spojených státech

- balancování potřeby ochrany investorů s podporou technologických innovací
- pozornost legislativy na federální i státní úrovni + dozorových orgánů (SEC, CFTC, FTC, IRS, FinCEN(=Financial Crimes Enforcement Network))
- absence federální úpravy X několik snah o úpravu v dílčích státech

- A) **podpora skrze úlevy a minimální požadavky** (např. Wyoming – vynětí z majetkové daně / Arizona – přijetí Bitcoin jako platidla pro daňové účely)

- B) **varování před riziky a důvěrou v kryptoměny** (např. Kalifornie či Nové Mexiko)

- C) **přijetí restriktivních pravidel** (např. New York)
- definice neuzavřené a flexibilní, pravidla často proměnlivá případ od případu

Přístup ve Spojených státech

- Diskutované regulatorní úrovně
- **Tržní regulace**
  - především pravidla a dozor proti manipulaci trhu, úprava futures a derivátových produktů
- **Právo cenných papírů**
  - SEC v. W.J. Howey Co. 328 U.S. 293, 301 (1946) – „investiční smlouva“ (investment contract)?
    - pozice SEC – pokud má token užitek = podléhá regulaci SEC, především jeho ICO
    - požadavek na licenci brokera u SEC, přípustnost obchodování pouze na fórech schválených SEC
- **AML, CTF a regulace finančních transakcí**
  - obecně se aplikují X fragmentovanost + složitá implementace ze strany FinCEN
- **Daňové právo**
  - IRS 2014 – zdaňitelné jako majetek nikoliv finanční prostředky
  - od 2018 zohlednění změny hodnoty investice pro účely daňové úlevy či přirážky
- **Dědické právo**
  - možná součást dědictví X závěti a odkazy nepraktické = neprávní nástroje přechodu účtů
  - potřeba technických instrukcí + soukromého klíče, jinak dědictví nedosažitelné
  - problémy: nevratnost transakcí, nezměnitelnost soukromého klíče (=potřeba uchování v tajnosti – trezor?), hard forks,air drops

Přístupy v dalších zemích

- Zdroj

- **Austrálie**
  - diskutováno od roku 2015
  - legislativní úpravy pro zabránění dvojího zdanění
  - 2017 – burzovní činnosti s kryptoměnami - AML/CTF legislativa dopadá
  - informování spotřebitelů a varování proti rizikům investiční spekulace

- **Čína**
  - nejsou přijímány jako platidlo, banky s nimi nesmějí nakládat
  - nezákonnost ICO, omezení činností směnáren
  - od 2018 - odrazování od podnikání formou těžby Bitcoin
  - pokračující pilotní provoz státem zřízené kryptoměny e-CNY , resp. DC/EP

Přístupy v dalších zemích

- **Japonsko**
  - 2017 – směnárenská činnost regulována, podléhající AML úpravě, ochraně spotřebitele, dozoru státního orgánu, registraci a bezpečnostním a ohlašovacím povinnostem srovnatelným s finančními institucemi
    - iniciátor = incident Bitcoinové směnárny Mt. Gox v roce 2014
    - systém otestován incidentem směnárny Coincheck v roce 2018 – reaktivní revize všech směnáren s kryptoměnami, 2 pozastavena činnost
  - Bank of Japan – 10/2020 – studie překážek pro tvorbu národní digitální měny

- **Švýcarsko**
  - kryptoměny klasifikovány jako aktiva = předmět vlastnického práva
  - příznivé podmínky pro fintech – „regulatorní sandbox“
    - státní dohled (Eidgenössische Finanzmarktaufsicht, FINMA)
  - regulace obecná, škálovatelná případ od případu
    - aplikace AML, podmínky ICO dle rozhodnutí FINMA
    - 2017 – FINMA zrušila provozovatele falešné kryptoměny E-Coin
  - zdanění – závislé na úpravě v daném kantonu

MUNI
LAW

Smart kontrakty

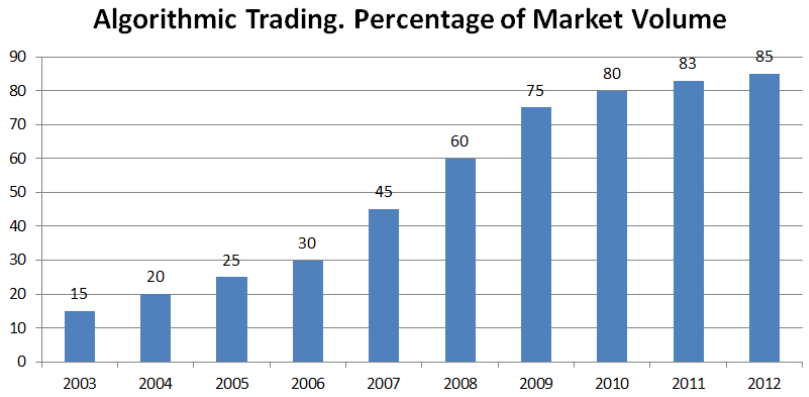
Obsah

Pojem a uplatnění

- Původ pojmu - Nick Szabo – 1996
- obecný koncept X rozšíření na platformě Ethereum skrze Ethereum virtual machine
- programovatelné protokoly s algoritmicky vyjádřenými záznamy smluvního ujednání
- soubor matematických pravidel + blockchain + nezměnitelnost + tokeny
    - tvorba (programovatelnost) => nasazení (vykonatelnost) => realizace (vymahatelnost)
    - „chytrý“ element spočívá v algoritmizaci určité povinnosti či jednání stanoveném v daném smluvním ujednání za pomoci kódu
- digitální zajištění transakce bez potřeby centrální autority pro vymožení plnění
- rozšíření aplikace konceptu blockchain na široké spektrum programovatelných transakcí
    - lze nastavit samovykonatelnost = nezrušitelnou aktivaci při splnění podmínek
    - lze nastavit samovymahatelnost = závazné provedení transakce fixací dotčených prvků
    - předpokládaný benefit = vyšší jistota transakce = snížení transakčních nákladů

Proto-chytré kontrakty

- automatizované obchodovací algoritmy
- srovnatelná programovací logika X bez vazby na blockchain
- Michael Lewis – Flash Boys: A Wall Street Revolt
- Vysokorychlostní obchodování (HFT)
- Finanční transakce – jednoduché, jednoznačné, kvantifikovatelné
- nastavení jednoznačných ukazatelů transakce



Ethereum Virtual Machine

- Platforma pro chytré kontrakty za pomoci kryptoměny Ethereum
- nezměnitelnost – nezávislost vymahatelnosti na jiných vlivech než vstupních parametrech
- Kirill Juran – „nákup v automatu“ – deterministický = neutrální
- „překladač“ mezi pokyny a programovacím jazykem
- *opcodes* = 140 unikátních pokynů – Turingově kompletní set
    - Stack-manipulating opcodes (*POP, PUSH, DUP, SWAP*)
    - Arithmetic/comparison/bitwise opcodes (*ADD, SUB, GT, LT, AND, OR*)
    - Environmental opcodes (*CALLER, CALLVALUE, NUMBER*)
    - Memory-manipulating opcodes (*MLOAD, MSTORE, MSTORE8, MSIZE*)
    - Storage-manipulating opcodes (*SLOAD, SSTORE*)
    - Program counter related opcodes (*JUMP, JUMPI, PC, JUMPDEST*)
    - Halting opcodes (*STOP, RETURN, REVERT, INVALID, SELFDESTRUCT*)
- *poplatek za smart kontrakt* – ochrana sítě před přetížením
- *constructor* – iniciační kód daného smart kontraktu na blockchainu
- *„oracles“* – vstupy třetí strany o externích podmínkách nezbytných pro naplnění parametrů smart kontraktu
- **uplatnění v ICO** = smart kontrakt jako závazná nabídka vůči investorům
- **uplatnění formou DAO** = komplextní formát – entita s nastaveným cílem a matematickými pravidly jednání
- **uplatnění formou DAPP =** decentralizovaná aplikace – open source, P2P, online distribuovaná služba

Očekávání spojovaná se smart kontrakty

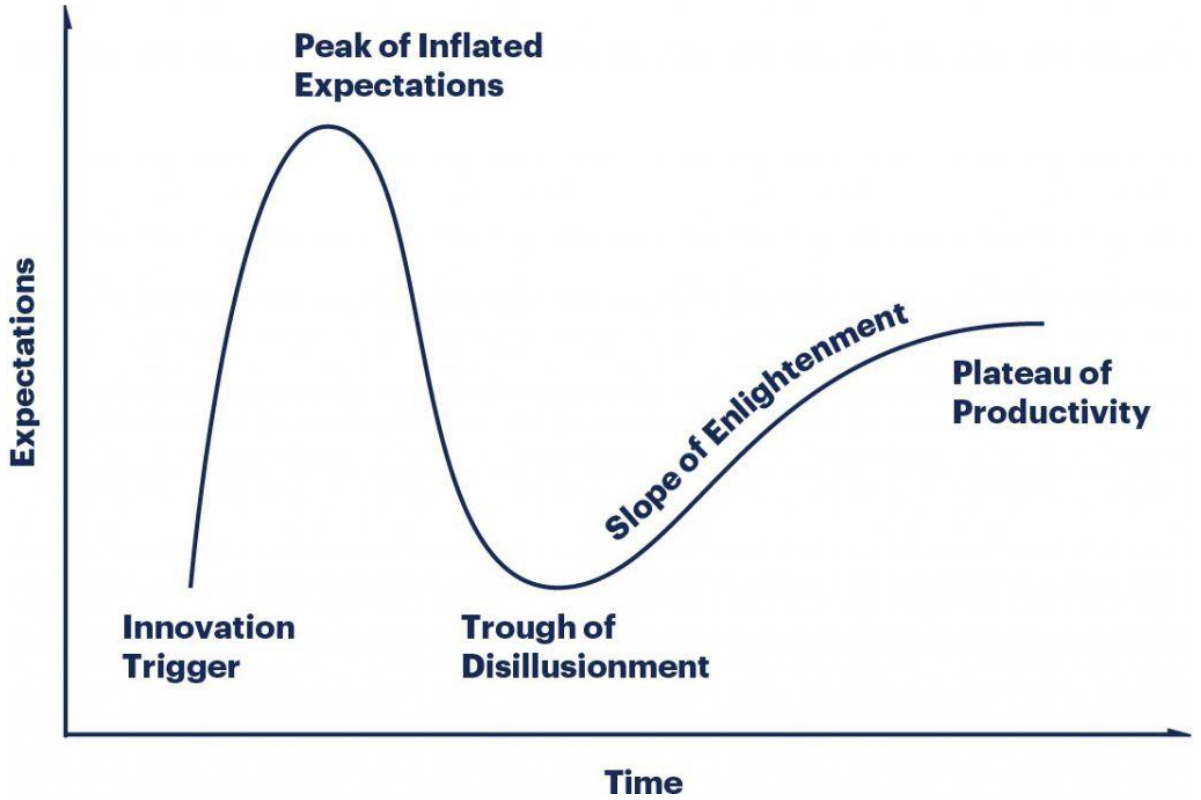
- Předpokládané úspory ve finančních transakcích
  - Příklad: Santander
  - Příklad: IKEA – chytrá fakturace
- Široká využitelnost při utváření nejrůznějších záznamů
  - Příklad: vytváření zdravotní dokumentace
- Převody nemovitostí
  - Příklad: Deloitte
- Pojišťovnictví a spory z pojištění
  - Příklad: Zpracování nároků
- Validace a dohledatelnost původu informace
  - Příklad: Ethereum

Smart kontrakty a virtualizace práva

- Limity zachycení právního obsahu do strojového kódu
- POLČÁK, R. *Internet a proměny práva*
  - Právo – požadavek předvědomí
- KNAPP, V. *Právo a informace*
  - „(…) *aby kybernetické zkoumání a zpracovávání kvantitativní stránky určité kvality bylo možné, musí být příslušná věda (a logika) způsobilá vyjádřit nutné předpoklady tohoto zkoumání konečným počtem konečných logickomatematických formulí, tj. způsobem ´srozumitelným´ kybernetickým strojům.*“
- Gödelovy věty o neúplnosti
- Projev vůle a omyl v právním jednání
- Smart kontrakt jako nástroj po uchování jednoznačného zachycení vyjádřené vůle
  - X právní problém je zpravidla právě dostatečně jednoznačné vyjádření vůle v právním smyslu
  - X právní formulace mohou být interpretovány na základě kontextových či dalších prvků jednání – smart kontrakt vyžaduje úplně zachycení eventualit či flexibilit výkladu již v původním zachycení = lze pouze pro velmi jednoznačné a jednoduché transakce
  - programovatelnost práva omezena jeho algoritmickou vyjádřitelností a praktickou užitečností jeho rigidního zachycení

Závěrečné myšlenky

- Hype vs. realita
  Potenciál vs. praktická aplikovatelnost



Vhodné zdroje pro hlubší studium problematiky

- dostupné v knihovně PrF MU:
  - BRUMMER, Chris (ed.). Cryptoassets: Legal, Regulatory and Monetary Perspectives. Oxford University Press. 2019, 441 s., ISBN: 9780190077327.
  - FOX, David; GREEN, Sarah (eds.) Cryptocurrencies in Public and Private Law. Oxford University Press. 2019, 323 s., ISBN: 9780198826385.
  - DĚDIČ, Jan; ŠOVAR, Jan; MIKULA, Ondřej. Proč podle českého soukromého práva nelze uvažovat o (ICO) tokenech jako o cenných papírech. Právní rozhledy. 2018, č. 15-16, s. 554–556.
  - NĚMEC, Libor; TORNOVÁ, Jarmila., K právní regulaci kryptoměn. Díl II. Právní rádce. roč. 2018, č. 7.
- dostupné online
  - JAREŠ, Adam. Kryptoměny a občanské právo. Revue pro právo a technologie. [online]. 2020, č. 21, s. 21-46. [cit. 2021-02-22]. Dostupné z: https://journals.muni.cz/revue/article/view/13216
  - KASL, František. Blockchain, společenská smlouva digitálního věku? Revue pro právo a technologie. [online]. 2018, č. 17, s. 3-18. [cit. 2021-02-22]. Dostupné z: https://journals.muni.cz/revue/article/view/8922
  - LEHDONVIRTA, Vili. The blockchain paradox: Why distributed ledger technologies may do little to transform the economy. Oxford Internet Institute [online]. 2016 [cit. 2021-02-22]. Dostupné z: https://www.oii.ox.ac.uk/blog/the-blockchain-paradox-why-distributed-ledger-technologies-may-do-little-to-transform-the-economy
  - SATOSHI NAKAMOTO. Bitcoin: A Peer-to-Peer Electronic Cash System [online]. 2008 [cit. 2021-02-22]. Dostupné z: https://bitcoin.org/bitcoin.pdf
  - SCLAVOUNIS, Odysseas. Understanding Public Blockchain Governance. Oxford Internet Institute [online]. 2017 [cit. 2021-02-22]. Dostupné z: https://www.oii.ox.ac.uk/blog/understanding-public-blockchain-governance
- další zdroje
  - LÁNSKÝ, Jan. Kryptoměny. 1. vydání. Praha: C. H. Beck, 2018.
  - STROUKAL, Dominik; SKALICKÝ, Jan. Bitcoin a jiné kryptopeníze budoucnosti. Praha: Grada. 2018.

MUNI LAW

Děkuji za pozornost!