KRYPTOMĚNY

Digitální výzva (nejen) pro právo

Právnická fakulta MUNI 27. listopadu 2019 Roman Šafář

MUNI LAW

Osnova přednášky

- **Kryptoměny** - pojem, stručná historie, základní principy fungování, obchodování s kryptoměnami (směnárny, burzy), příklady nejznámějších kryptoměn v současné době
- **Blockchain** - DLT, P2P sítě - jejich (současné i budoucí) využití
- **Smart Contracts**
- **Tokeny**

+ příběh z Afriky

KRYPTOMĚNY

MUNI
LAW

Vymezení pojmu

- Negativní definice: Vymezení vůči bezhotovostním penězům a fiat měnám
- Pozitivní definice:
  - **Digitální měna**, která funguje na základě šifrovací technologie.
  - Existuje **protokol** („zákon dané kryptoměny“), na jehož základě se kryptoměna vytváří a na jehož základě probíhají transakce s danou kryptoměnou.
  - Pravidla vzniku, fungování a obchodování dané kryptoměny jsou **nezávislá na centrální instituci**, a to díky DLT, zejména technologie blockchain.

Reakce českého zákonodárce

- V ČR chybí zákonná definice i regulace kryptoměn
  - Zatím pouze veřejné konzultace za účelem regulace ze strany Ministerstva financí ČR (nehmotná věc v právním smyslu) a 3 stanoviska ČNB (o obchodování s bitcoiny; o regulaci investičních fondů a tzv. ICOs; k obchodování s převodními tokeny)
- Zahraniční inspirace - Malta, Lichtenštejnsko, Japonsko, USA
  - M: Balíček 3 zákonů z 22. 5. 2018: (1) regulace společností obchodující s kryptoměnami (krypto-směnárny ad.); (2) regulace pro ICO; (3) zřízení regulačního úřadu dohlížejícího na dodržování standardů a doporučení ve vztahu ke kryptoměnám a DLT
  - L: Zákon o tokenech a entitách poskytujících služby založené na důvěryhodných technologiích
- Čekat na EU, nebo regulovat na národní úrovni?

Základní pilíře kryptoměn

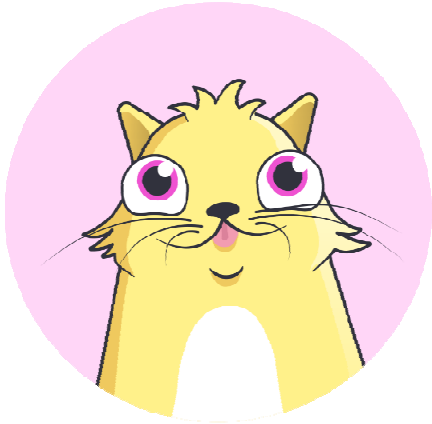
- **Decentralizace** a **bezpečnost**
  - Státní „kryptoměna“? (neúspěch Petra ve Venezuele)
  - Kryptoměna krytá fiat měnou - Tether krytý USD
  - Kryptoměna navázaná na komoditu - kávu (Coffee - Kolumbie)
- **Důvěryhodnost** a **(právní) jistota**
  - Protokol a jeho další směřování na základě konsenzu zúčastněných
- **Transparentnost**
  - Otevřený kód

Kryptoměny - historický vývoj

- 0. generace: 2009, Satoshi Nakamoto, **Bitcoin**
  - *Proof of work* (vynaložení počítačového výkonu za odměnu v podobě Bitcoinu) = bezpečné (potvrzování transakcí všemi zúčastněnými), ale energeticky náročné

- I. generace: **altcoiny** (Litecoin, Bitcoin Cash, Monero a Zcash)
  - Hledání alternativ k Bitcoinu a jeho vlastnostem
  - *Proof of stake* (čím víc těžené kryptoměny již držím, tím větší dostanu odměnu za vykonanou těžbu, či za množství potvrzených transakcí) → vlastníci kryptoměny jsou tedy motivováni ji i používat při transakcích
  - Monero a Zcash - anonymita (NE pseudonymita) díky šifrovacím protokolům - např. skryté adresy (tajné, jednorázové adresy příjemců)

Kryptoměny - historický vývoj



- II. generace: **Ethereum** (platforma i kryptoměna)
  - Platforma umožňující vytváření smart contracts a tokeny
  - Hry: *cryptokitties* (vznik virtuálních koček za pomoci SC, uložených do blockchainu, možný jejich prodej a další křížení - některé prodány i za /v přepočtu/ 115 000 USD)

- III. generace: **Cardano** (platforma) + **ADA** (kryptoměna)
  - Využití (delegovaného) *Proof of Stake* – volí se zástupci na určitou dobu, kteří budou potvrzovat transakce.
  - Racionalizace využívání kryptoměn a DLT - ořezávání nepotřebných částí v blocích, zmenšení objemu dat, dělení dat uchovávaných jednotlivými uzly/uživateli (+ vzájemné propojení a zálohování) → nižší energetická náročnost.

Obchodování s kryptoměnami

- Krypto-burzy, krypto-směnárny, směny a obchody v rámci „krypto-komunity“, bitcoinmaty (bitcoin bankomaty)
- ICO („primární nabídka *coins*“) - *white paper* (emisní podmínky, ve kterých je mj. informace o dané kryptoměně, o směřování kryptoměny a další informace pro /potenciální/ investory)
- Peněženky (základní druhy):
  - Mobilní / desktopové - aplikace na mobilu (př. Coinomi, Jaxx) / PC
  - Webové
  - Hardwarové (př. Trezor)
  - Papírové - vytištěný soukromý klíč a veřejný klíč
  - + full node - počítač je zároveň uzlem („těží“) a zároveň peněženkou

Obchodování s kryptoměnami

- Jak investovat? Základní doporučení: **diverzifikace rizika**
  - Více kryptoměn na jedné krypto-burze/krypto-směnárně
  - Více kryptoměn ve více krypto-burzách/krypto-směnárnách
  - Jednu kryptoměnu na více krypto-burzách/krypto-směnárnách

Využití kryptoměn

- Platidlo - záleží na typu transakce (zejména objemová podmínka)
  - **„Malé“ transakce** (nákup zboží každodenní spotřeby; př. potraviny) - **nevyplatí se**, neboť hodnota transakčních nákladů (zejména jednotka času, za kterou bude transakce ostatními uzly potvrzena) je vyšší než hodnota samotného zboží
  - **„Velké“ transakce** (př. automobil) - pokud není požadavek na rychlost transakce, což typicky není, **vyplatí se** využít kryptoměnu

- Investiční nástroj – holdeři, spekulanti

Rizika a nevýhody spojená s kryptoměnami

- Malý objem a pomalost transakcí - jak zrychlit transakce (PoS, Cardano) za současného snížení energetické náročnosti?
  - Paradox: koupě 2 pizz za 10 000 BTC (41 USD) - *Bitcoin pizza day* (2010)
- Energetická náročnost při těžbě - negativní dopady na životní prostředí
  - Těžit individuálně, nebo kolektivně (v *těžebních poolech* – Slush Pool (Marek Palatinus)?
- Nové trestné činy a/nebo nové podoby stávajících trestných činů
  - Krádež kryptoměny - vykradení peněženky, vykradení krypto-směnárny/burzy (*hot wallet*)
  - Krach burzy Mt. Gox (konec 2013) → snížení hodnoty BTC
  - Silk Road - Ross Ulbricht (2013)

Nejznámější současné kryptoměny

- Bitcoin
- Bitcoin Cash - *hard fork* v důsledku „války o blok“ (o velikost bloku)
- Ethereum
- Ethereum Classic
- Litecoin
- Zcash, Monero - anonymita (NE pseudonymita) díky šifrovacím protokolům - např. skryté adresy (tajné, jednorázové adresy příjemců)

TOKENY

MUNI
LAW

Tokeny

- Jejich role v rámci krypto-světa
- Fungují v rámci blockchainu dané kryptoměny (zejména Etherea), nikoli samostatně.
- ITO („primární nabídka tokenů“) – *white paper* (emisní podmínky, ve kterých je mj. informace o právech spojených s daným tokenem a další informace pro /potenciální/ investory)
- Jsou cennými papíry (dle českého práva)? - nezávislost VP a SP
  - Soukromoprávní odpověď - NE
  - Veřejnoprávní odpověď - ANO i NE

Druhy tokenů

Dělení na základě ekonomické podstatě tokenů:

- **Security token** (*asset token*, *investment token*)
  - Velmi podobné jako investiční cenné papíry - účast investora na projektu
  - Lze s nimi spojit různá práva - podíl na zisku, hlasovací práva atp.
- **Utility token**
  - „voucher“
  - Možnost (digitálního) přístupu ke zboží nebo službě projektu, který investor finančně podpořil
  - Absurdní příklad - *sociální síť Steemit*
- **Currency (payment) token**
  - Platidlo, platební prostředek, „kryptoměna v užším smyslu“

Soukromoprávní pojetí

– Definice CP v § 514 OZ:

„Cenný papír je listina, se kterou je právo spojeno takovým způsobem, že je po vydání cenného papíru nelze bez této listiny uplatnit ani převést.“

– Požadavky na CP vyplývající ze (soukromoprávní) definice:

1. projev vůle emitenta zachycený na **hmotném** substrátu
2. inkorporované právo nelze bez předložení hmotného substrátu **uplatnit**, ani **převést**

Soukromoprávní odpověď

- Tokeny nejsou zaznamenány, ani zaznamenatelné na hmotném substrátu X vyloučena možnost považovat CP za elektronickou písemnost dle § 562 OZ.
- CP nelze ani konvertovat do elektronické podoby dle zákona (č. 300/2008 Sb.) o elektronických úkonech a autorizované konverzi dokumentů.
- Tokeny nejsou ani CP (dle § 514 OZ), ani zaknihovanými CP (dle § 525 OZ).

Veřejnoprávní pojetí

- Investiční nástroje (§ 3 odst. 1 písm. a) ZPKT) → investiční cenné papíry (§ 3 odst. 2 ZPKT)
- Znaky investičních cenných papírů:
    1. formální kritéria - **obchodovatelnost** a **převoditelnost**
    2. materiální kritérium - **povaha inkorporovaných práv**

Veřejnoprávní odpověď

- Security (asset) tokeny by mohly být považovány za investiční cenné papíry, pokud by:
  - Byly obchodovatelné na kapitálovém trhu
  - Byly převoditelné (i omezeně?)
  - V nich byla inkorporována taková práva, která by plnila primárně **investiční funkci** (např. právo na podíl na zisku, právo na předem určený výnos, hlasovací práva v rámci daného projektu - emitenta).

BLOCKCHAIN

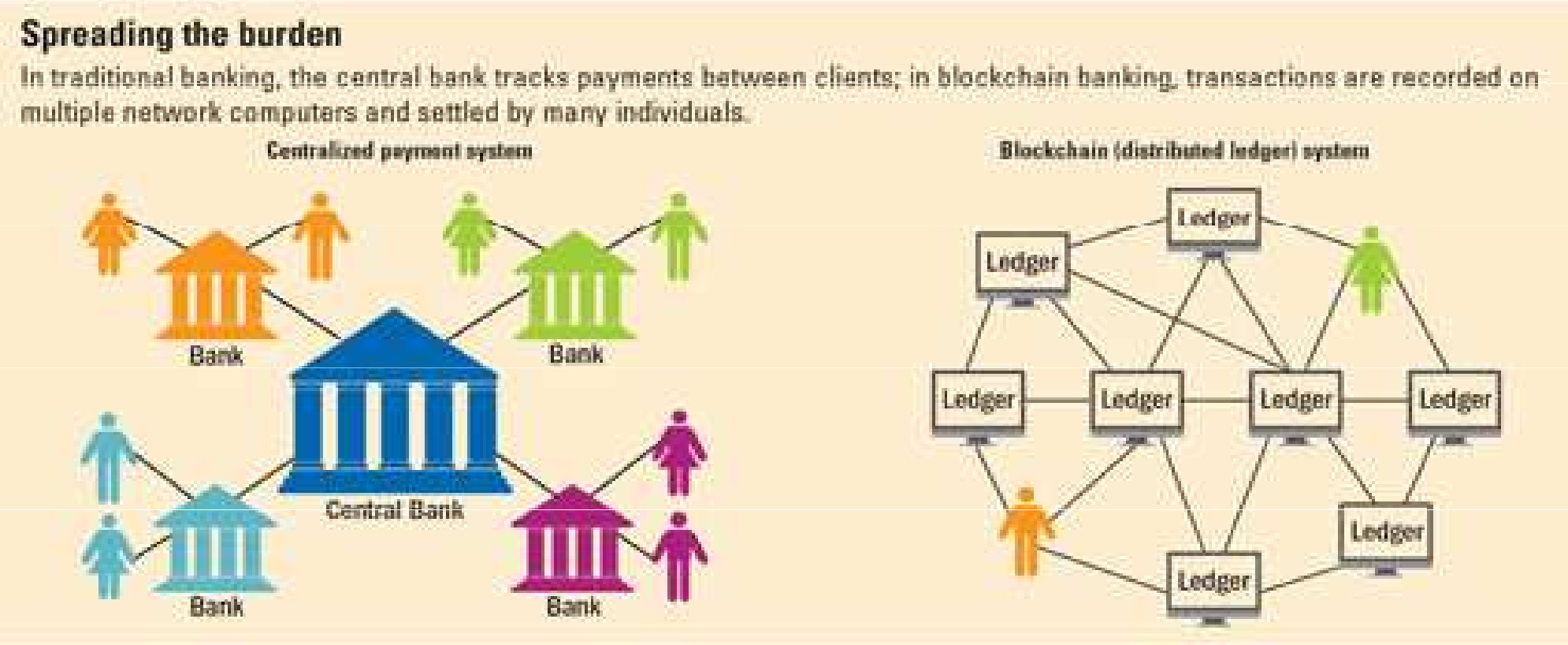
MUNI
LAW

Blockchain

- Nejznámější zástupce DLT (*distributed ledger technology*)

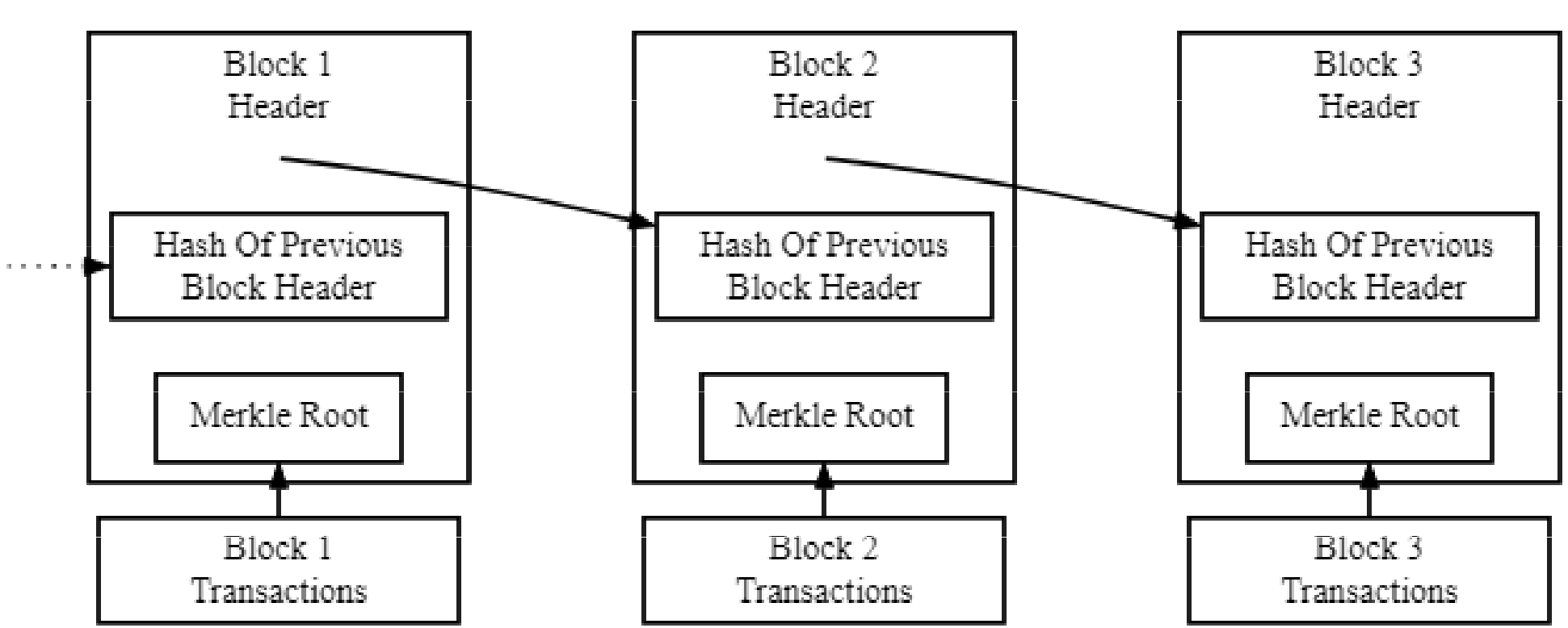
- Databáze, která zaznamenává a uchovává údaje o veškerých transakcích. Navíc je u každého zúčastněného uchována kopie daného blockchainu v určitém časovém okamžiku.
- Znemožnění podvodných transakcí → k provedení transakce je nutný konsensus zúčastněných

Princip fungování



MUNI LAW

Schéma blockchainu



Simplified Bitcoin Block Chain

LAW

Současné i budoucí využití DLT technologií

- Trh s cennými papíry a komoditami – záznamy o vlastnickém právu k CP a komoditám
- Katastr nemovitostí – záznamy o vlastnickém právu k evidovaným nemovitostem
- Zápůjčky finančních prostředků

- a mnoho dalších oblastí…

SMART CONTRACTS

MUNI
LAW

Co je na SC „smart“?

- Co je SC? Není to smlouva, je to jakýsi doplněk, „přívěsek“ ke smlouvě „hlavní“
  - Př. automat na kávu (bude-li vhozena dostatečně vysoká částka peněz, dostaneme kávu X dostaneme peníze zpět); crowfunding (bude-li vybrána požadovaná výše finančních prostředků,
- Fungují samostatně (→ samovykonatelnost) na základě předem definovaných kritérií v protokolu.
- Lze tak snadno financovat nový podnikatelský projekt - startup - za pomoci crowdfundingu.

Výhody a nevýhody SC

- Pro pořizovatele SC - nemusí hlídat splnění dluhu protistrany
- Univerzálnost - může být využitelný pro více stejných závazkových vztahů
- Pro druhou stranu závazkového vztahu - vyšší míra právní jistoty v případě nesplnění podmínek druhé strany
- Vyšší nároky při jeho vytvoření, resp. zadání vytvoření
- Vysoké pořizovací náklady (IT specialisté)
  - Odvíjí se od předmětu závazku, objemu závazku atp.

Legislativní výzvy (nejen) pro českého zákonodárce

- Už dnes: Povinnost identifikovat klienta, který provádí transakci nad 1000 € (§ 7 AML zákona) + zejm. pro security tokeny právní úprava investičních nástrojů, konkr. investičních CP (§ 3 ZPKT)
- V budoucnu:
  - Legislativní vymezení (definice) kryptoměn a DLT
  - Trestněprávní důsledky
  - Důsledky na životní prostředí
  - Ochrana spotřebitele
  - Dědění peněženek
- Čekat na EU, nebo regulovat na národní úrovni?

BONUS: Příběh z Afriky

m-pesa

MUNI
LAW

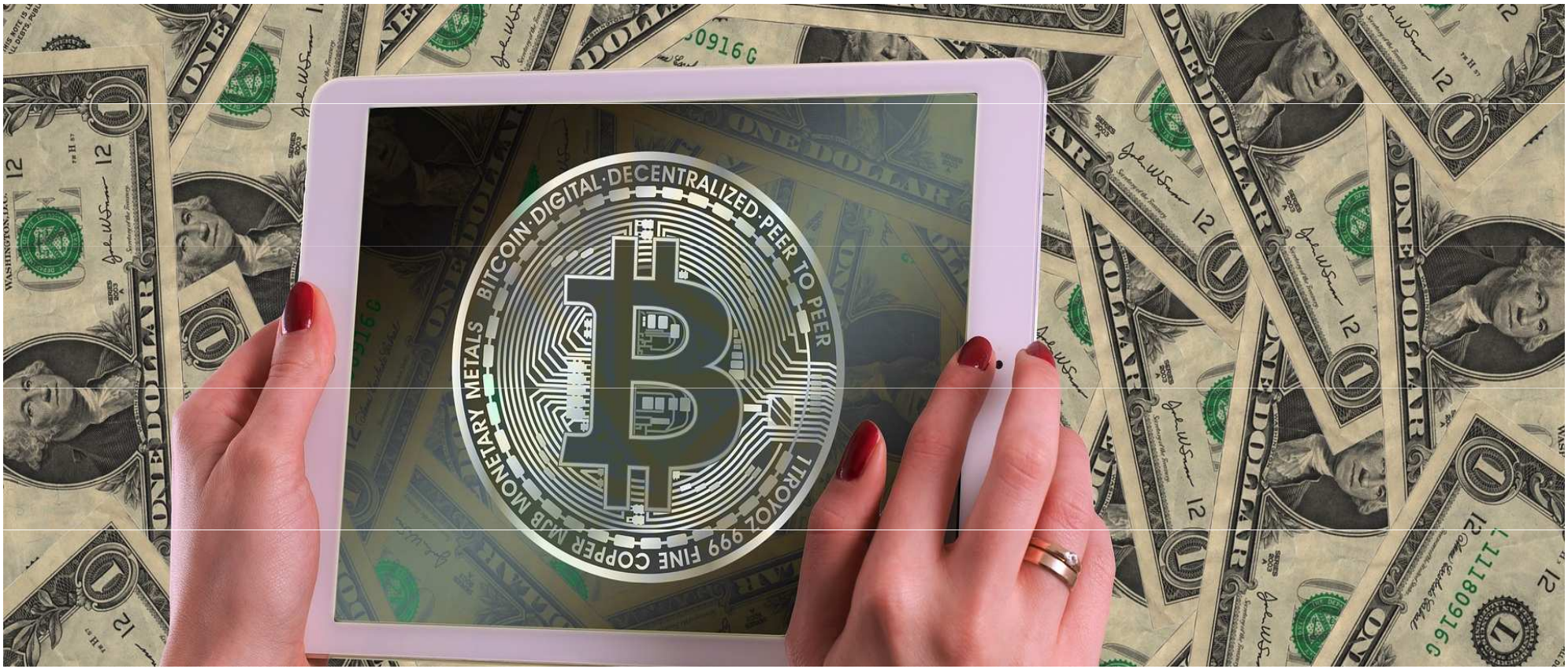
MUNI
LAW

Máte dotazy?

Osobně - teď

E-dotazy - kdykoli na 427148@mail.muni.cz

Děkuji Vám za pozornost



MUNI
LAW