https://doi.org/10.5817/RPT2018-1-1

BLOCKCHAIN, SPOLEČENSKÁ SMLOUVA DIGITÁLNÍHO VĚKU?

FRANTIŠEK KASL[1]

ABSTRAKT

Příspěvek nabízí stručné pojednání o nalézání legitimity definiční autority skrze teorii společenské smlouvy aplikovaném na prostředí technologie blockchain. Po úvodním shrnutí historického vývoje tohoto zásadního teoretického konceptu je pozornost zaměřena na limity, které mu jsou vystavovány v prostředí kyberprostoru. Následně je zmíněna role definičních autorit a jejich význam v tomto kontextu. Pozornost se pak již přesouvá na technologii blockchain, jakožto možný inovativní legitimační model vhodně kombinující požadavek na implicitní podporu většiny s potřebou výkonu autoritativní moci skrze mechanismus s reálným dosahem na dané prostředí. Po rozboru systému vytváření důvěry, změny definičních norem a organizaci podílu na autoritativním výkonu moci v rámci této platformy je však formulován názor, že tato nová technologie, sice přenáší problém legitimity na novou úroveň, ale v jeho vlastní podstatě jej neřeší.

KLÍČOVÁ SLOVA

Společenská smlouva; definiční autorita; blockchain

ABSTRACT

The contribution provides a short treatise on search for legitimacy of the definition authority through the theory of social contract applied on the environment

[1] Mgr. Ing. František Kasl je prezenčním doktorským studentem na Ústavu práva a technologií Právnické fakulty Masarykovy univerzity v Brně. Kontaktní e-mail: frantisek.kasl@mail.muni.cz.

of the blockchain technology. Pursuant to the introductory summary of the historical evolution of this crucial theoretical concept is the attention focused on limits, which are for it created in the cyberspace environment. Next is mentioned the role of definition authorities and their significance in this context. Focus is afterwards shifted to the blockchain technology, as a potential innovative legitimacy model, which amply combines the requirement of implicit support by the majority with the need for exercise of authoritative power through a mechanism with a real impact on the given environment. Based on an analysis of the system of creating trust, changing definition norms and organisation of the share on authoritative exercise of power within this platform, an opinion is formulated that this new technology may on one hand transfer the issue of legitimacy to a new level; however it does not solve it in its own nature.

KEYWORDS

Social contract; definition authority; blockchain

1. ÚVOD

Legitimita autoritativního výkonu moci je dlouhověkým předmětem politicko-filozofického diskursu.[2] S příchodem kyberprostoru vyvstala pro toto nalézání ospravedlnění pro organizační uspořádání společnosti nová výzva v podobě online prostředí, která vede k rostoucímu významu definičních autorit soukromoprávního charakteru, jakožto subjektů, které mají reálnou kapacitu vymáhat státem vymezená práva a povinnosti. Specifickým alternativním modelem uspořádání, slibujícím ideologické osvobození od mocenských struktur, je v současné době hojně diskutovaný koncept blockchainu, neboli decentralizované kryptograficky podložené databáze záznamů, která umožňuje provádět široké spektrum operací bez potřeby centrální autority zajišťující důvěru a upravující pravidla mechanismu.[3] Předmětem

[2] K historickému diskursu ohledně právního řádu jako systému legitimaci výkonu moci viz např. TAMANAHA, Brian Z. *On the Rule of Law: History, Politics, Theory*. Cambridge: Cambridge University Press, 2004. či CANEVARO, Mirko. *The Rule of Law as the Measure of Political Legitimacy in the Greek City States* [online]. 2017 [vid. 15. březen 2018].

[3] Pro více o konceptu viz např. The great chain of being sure about things. *The Economist* [online]. 2015 [vid. 15. březen 2018].

tohoto stručného pojednání je úvaha nad legitimitou autonomní organizace, kterou tento koncept slibuje v porovnání se standardnějšími formami definiční autority.

2. SPOLEČENSKÁ SMLOUVA JAKO ZÁKLAD LEGITIMITY AUTORITATIVNÍ MOCI

Otázky týkající se platnosti, legitimity a vymahatelnosti práva v prostředí kyberprostoru směřují k samotnému právně-teoretickému jádru podstaty práva a autoritativního vynucování moci. Nelze tedy odhlédnout od formujících myšlenek teorie společenské smlouvy, které lze pokládat za legitimační základ západního vnímání společenského uspořádání. Lze přitom do značné míry protnout myšlenky původně formulované Thomasem Hobbesem v jeho klíčovém díle *Leviathan*[4] s do značné míry oponujícími tezemi jeho současníka Johna Locka představenými v díle *Druhé pojednání o vládě*.[5] Přestože každý z těchto politických filozofů nahlížel na koncept implicitní společenské smlouvy mezi členy společnosti o jejím uspořádání a organizaci z odlišného pohledu a sledoval v ní odlišný účel, nelze opominout koncepční blízkost a shodný základ obou tezí, tedy implicitní ospravedlnění výkonu autoritativní moci skrze předpokládaný prospěch pro jednotlivce i společnost jako celek. V podobném duchu rozvinul myšlenku o století později i Jean-Jacques Rousseau v díle *O společenské smlouvě neboli zásadách státního práva*.[6]

Myšlenky tohoto legitimačního nástroje byly následně vyvíjeny s přispěním řady významných myslitelů novověku. Moderní pojetí teorie společenské smlouvy nabídl ve svém díle *A Theory of Justice*[7] John Rawls, kde protíná principy rovnosti a svobody ve snaze nalézt nástroj zajišťující proporcionální či distributivní spravedlnost ("*distributive justice*"). Centrální maximy jeho díla pak jsou, že každé osobě by se mělo dostat nejširšího sou-

[4] HOBBES OF MALMESBURY, Thomas. *Leviathan* [online]. 1651 [vid. 15. březen 2018].

[5] LOCKE, John. *Druhé pojednání o vládě*. Přel. KRÁL, Josef. Praha: Svoboda, 1992 (1689).

[6] ROUSSEAU, Jean-Jacques. *O společenské smlouvě neboli zásadách státního práva*. Plzeň: Aleš Čeněk, 2002 (1762).

[7] RAWLS, John. *A Theory of Justice*. Cambridge, Massachusetts: Belknap Press of Harvard University Press, 1971.

boru základních svobod, který daný systém může nabídnout, a současně, že sociální a ekonomické nerovnosti mají být vázány na funkce dostupné všem za podmínek spravedlivé a rovné příležitosti a při jejich řešení musí být kladen největší důraz na zlepšení pozice nejvíce znevýhodněných.[8] V reakci na toto dílo vydal Robert Nozick své teze *Anarchy, State, and Utopia*[9] o potřebě minimálního státu, jakožto cesty k nejmenší míře omezování přirozených práv a svobod členů společnosti a přirozeném organizačním výsledku anarchie. V jeho argumentech se odráží řada konceptů, které činí zmiňovaný mechanismus blockchain atraktivním nástrojem pro zajištění maximální míry svobody v online prostředí.

3. PROBLÉM VYMAHATELNOSTI PRÁVA NA INTERNETU

Výše představený koncept legitimizace autority narazil na nové překážky a výzvy při vstupu lidské společnosti do doby digitální, která se s rostoucí měrou odehrává v prostředí kyberprostoru. V této virtuální dimenzi utvářené komunikačními a informačními technologiemi se znovu otevřela diskuse o legitimní distribuci moci, především s ohledem na proměnu některých faktorů, které činili dosavadní struktury ve vymáhání své autoritativní vůle značně neúčinné.

V kyberprostoru předně dochází k zásadnímu oslabení faktoru polohy a vzdálenosti, jelikož informace jsou přenášeny formou datových paketů přes páteřní sítě v zásadě bez ohledu na teritoriální příslušnost dané infrastruktury.[10] Rychlost a frekvence datových přenosů dále v podstatě znamenala vypuštění faktoru vzdálenosti, do kontaktu tak dnes přicházejí nesčetné kombinace subjektů bez ohledu na jejich aktuální teritoriální příslušnost. Rozvoj internetové komunikace dále zesiluje její složitost, což se projevuje např. vzestupem cloudových služeb, které ze své podstaty tvoří provázaný systém datových toků mezi datovými servery rozmístěnými v různých

[8] *Tamtéž*, str. 266-267.

[9] NOZICK, Robert. *Anarchy, State, and Utopia*. New York: Basic Books, 1974.

[10] K podrobnějšímu popisu struktury internetové sítě a jejímu vývoji, včetně systému datových paketů na základě TCP/IP protokolů a konceptu síťové neutrality viz např. PASTOR-SATORRAS, Romualdo; VESPIGNANI, Alessandro. *Evolution and Structure of the Internet: A Statistical Physics Approach*. Cambridge: Cambridge University Press, 2007.

částech světa a cílovými zařízeními uživatelů v místě, kde se momentálně nacházejí.[11]

Nelze nadto opominout, že specifikem kyberprostoru je taktéž vysoká závislost jeho vnitřní logiky na lidské úvaze. Jedná se o prostředí, jehož základní zákonitosti byly vyvinuty za pomoci lidského úsudku a zůstávají alespoň v teoretické rovině předmětem lidské volby, neboť limity toho, co je či není v tomto prostoru možné, v zásadě určují stanovené parametry základních protokolů a uspořádání přenosové infrastruktury srovnatelně s tím, jak je to u zákonů přírodních při určování chodu světa reálného. V tomto duchu lze alespoň vnímat myšlenky představené Lawrencem Lessigem v díle *Code and Other Laws of Cyberspace*,[12] když argumentuje limity tradiční státní regulace internetu specifiky online prostředí, které je regulováno nejen právem, ale především architekturou prostředí, zvolenými technickými normami a tržními mechanismy.

4. ROLE DEFINIČNÍCH AUTORIT A JEJICH ODPOVĚDNOST ZA VYMAHATELNOST PRÁVA NA INTERNETU

Představy o svobodném a samoregulujícím se prostředí internetu shrnuté v *Deklaraci nezávislosti kyberprostoru*[13] však v posledních dekádách narážejí na rostoucí zásadní společenské problémy plynoucí z volnosti, otevřenosti a reálné nekontrolovatelnosti řady zákoutí tohoto digitálního prostoru. Závažnost problémů sahajících od projevů nenávisti přes masové porušování autorských práv až po závažné formy trestné činnosti konané skrze „podloubí" internetu[14] značí potřebu vykonavatelného působení regulátora, který v těchto ohledech má stále v zásadě podobu státu legitimovaného k výkonu autoritativní moci skrze zmíněné implicitní úvahy o společenské

[11] Podrobně o cloudových službách pojednává např. ANTONOPOULOS, Nick; GILLAM, Lee. *Cloud Computing: Principles, Systems and Applications*. Londýn: Springer, 2017.

[12] LESSIG, Lawrence. *Code and Other Laws of Cyberspace*. New York: Basic Books, 1999.

[13] BARLOW, John Perry. A Declaration of the Independence of Cyberspace. *Electronic Frontier Foundation* [online]. 8. únor 1996 [vid. 15. březen 2018]. Získáno z: https://www.eff.org/cyberspace-independence

[14] Tato část internetové sítě je často označována jako „dark web". Blíže viz např. CHERTOFF, Michael. A public policy perspective of the Dark Web. *Journal of Cyber Policy* [online]. 2017, roč. 2, č. 1.

smlouvě. K nezbytnosti rostoucí míry regulatorní kontroly státu nad prostředím internetu ostatně dospívá i Lawrence Lessig ve svém pozdějším díle *Code: Version 2.0*,[15] kde částečně opouští své předchozí teze o možnosti regulace pouze skrze technické normy (především protokoly a zdrojový kód) a připouští nevyhnutelnost potřeby účinného státního zásahu.

Za pragmatické vyústění této potřeby lze považovat využití mezičlánku v podobě definičních autorit různých segmentů kyberprostoru k delegovanému výkonu stále větší části autoritativní role státu nad online prostředím, jelikož tyto subjekty mají na rozdíl od státu ve vymezeném rozsahu své působnosti reálný dosah na přenos, vytváření, ukládání a zpracovávání informací na internetu a ze své zásadně soukromoprávní povahy mohou účinněji reagovat, neboť nejsou limitovány enumerativností veřejnoprávních pretenzí.

Pojem definiční autority označuje subjekt způsobilý ovlivňovat pravidla prostředí své působnosti. Tato pravidla lze označovat za definiční normy, a jejich přítomnost je nezbytná pro uspořádání každého logického systému, ať už se jedná o přírodní zákony světa kolem nás, či právní řád jakožto pravidla daného společenského systému.[16] V kyberprostoru je kontrola nad těmito pravidly roztříštěna mezi plejádu subjektů sahající od organizací typu ICANN (*Internet Corporation for Assigned Names and Numbers*)[17] po poskytovatele služeb informační společnosti nejrůznějších úrovní a funkcí.

Pod poskytovateli služeb informační společnosti (zkráceně *ISP* z *information service provider*)[18] lze zahrnout subjekty poskytující, zpravidla za úplatu, různé formy služeb online, např. hostingové služby, e-mailové portály, indexové vyhledávání, komunikační portály, sociální sítě, zpravodajské servery, datová úložiště či samotný provoz komunikační infrastruktu-

[15] LESSIG, Lawrence. *Code: Version 2.0*. New York: Basic Books, 2006.

[16] POLČÁK, Radim. *Internet a proměny práva*. Praha: Auditorium, 2012. str. 137-139.

[17] Viz ICANN. Welcome to the global community! *icann.org* [online]. [vid. 15. březen 2018]. Získáno z: https://www.icann.org/get-started

[18] Vymezení služby informační společnosti v současné době poskytuje směrnice 2015/1535 ze dne 9. září 2015 o postupu při poskytování informací v oblasti technických předpisů a předpisů pro služby informační společnosti, která nahradila směrnici 98/34/ES obsahující srovnatelnou definici.

ry.[19] Díky dosahu těchto subjektů na dílčí složky kyberprostoru, ve kterých má stát problém realizovat svou autoritativní moc, dochází k vynucování určité formy a míry regulace online jednání skrze rozšiřování (spolu)odpovědnosti těchto ISP za nezákonná jednání v online prostředí, kde působí jako definiční autorita.[20]

Tímto je sice pragmaticky dosahováno vyšší vymahatelnosti práva, avšak pouze za současného omezení práv daných soukromoprávních definičních autorit (skrze dovození jejich spoluodpovědnosti za jednání uživatelů jejich služeb) a za současného faktického přenosu části státní moci (např. výkladu přípustného a nepřípustného jednání) na soukromoprávní (a často komerční) subjekt. Není tedy překvapivá snaha o nalezení alternativního uspořádání, které by blíže reflektovalo koncept společenské smlouvy a omezovalo centralizovanou autoritativní moc určitého subjektu v pozici definiční autority.

5. ALTERNATIVA V PODOBĚ BLOCKCHAIN?

Na podzim roku 2008 bylo zveřejněno odborné pojednání[21] anonymního autora pod pseudonymem Satoshi Nakamoto, které popisovalo v teoretické rovině propojení řady ověřených principů pro vytvoření digitální distribuované účetní knihy. Ta měla zajišťovat důvěru v záznamy za pomoci kombinace kryptografie a decentralizované distribuce, čímž slibovala specifický model organizace bez centrální definiční autority, která by byla nahrazena zákonitostmi zdrojového kódu utvářeného vůlí většiny uživatelů. Na této koncepci byla vystavěna první kryptoměna Bitcoin. Rostoucí povědomí o koncepčních základech tohoto modelu však přináší stále více variací

[19] POLČÁK, Radim. *Internet a proměny práva*. Praha: Auditorium, 2012. str. 142.

[20] Podrobně se touto problematikou zabýval HUSOVEC, Martin. *Zodpovednosť na internete podľa českého a slovenského práva* [online]. CZ.NIC. Praha: CZ.NIC, 2014 [vid. 24. srpen 2017]. Za současný významný příklad užití tohoto postupu „delegované regulace" lze označit od nedávna účinný německý zákon pro zlepšení prosazování práva v prostředí sociálních sítí (*Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken* (*Netzwerkdurchsetzungsgesetz - NetzDG*)) ze dne 30. 6. 2017, č. 536/17. Dostupný např. z: http://dipbt.bundestag.de/dip21/brd/2017/0536-17.pdf

[21] SATOSHI NAKAMOTO. *Bitcoin: A Peer-to-Peer Electronic Cash System* [online]. www.bitcoin.org. 2008 [vid. 15. březen 2018].

uplatnění daleko za hranicemi původně zamýšleného autonomního platebního nástroje. Přestože řada užití poukázala na značné limity původního modelu, ústřední nosná myšlenka se projevila být dostatečně přizpůsobivá a inovativní, aby umožnila zrod nepřeberného množství více či méně životaschopných adaptací.[22]

Odhlédneme-li od technických parametrů konkrétní formy uplatnění i od ideologických (anarchisticky zabarvených) tezí původního pojednání, je možné se ptát, zda v této struktuře nedochází k jistému prolínání představy o společenské smlouvě legitimující definiční autoritu a formy vhodné pro prostředí kyberprostoru. Jinými slovy, lze blockchain považovat za inovativní legitimační model vhodně kombinující požadavek na implicitní podporu většiny s potřebou výkonu autoritativní moci skrze mechanismus s reálným dosahem na dané prostředí?

V rámci snahy o zodpovězení této otázky nahlédněme hlouběji nejprve do procesů utvářejících legitimitu a důvěru a následně do nástrojů, které umožňují proměnu pravidel a parametrů prostředí daného blockchainu.

6. TVORBA DŮVĚRY ZA POMOCI BLOCKCHAINU

Blockchain je postaven na bázi *peer-to-peer* sítě, tedy komunikační platformy propojující přímo cílová zařízení uživatelů bez využití centrálního či distribučního serveru. Jeho základní struktura spočívá v uchovávání celé historie záznamů ve všech těchto zařízeních a sofistikovaném využití šifrování k zajištění, že většina uživatelů bude v zásadě vycházet z těch záznamů o předchozím vývoji, které jsou nejvíce důvěryhodné. Tato důvěryhodnost je zajištěna kombinací autorizace stran za pomoci digitálních podpisů a současného provázaného šifrování jednotlivých bloků, které uchovávají záznamy. Bez ohledu na konkrétní způsob vytváření bloků dochází k jejich pravidelnému řetězení, které za pomoci asymetrického šifrování (především SHA-256) činí snahu o přidání neautorizovaného zázna-

[22] Pro přehled některých nadějných užití v širším prostředí finančních služeb viz např. KASL, František. European Smart Regulation of the Distributed Ledger Technology in the Financial Sector. In: SCHWEIGHOFER, Erich et al. (eds.) . *Trends and Communities of Legal Informatics IRIS 2017 Proceedings of the 20th International Legal Informatics Symposion*. Vídeň: Oesterreichische Computer Gesellschaft, 2017.

mu v dostatečně krátkém časovém horizontu vysoce nerentabilní a tudíž nepravděpodobnou.[23]

Z hlediska legitimity je atraktivní, že mechanismus nemá zjevnou centrální definiční autoritu, ale stanoví oprávněnost vnitřních pravidel skrze aktivitu širokého spektra uživatelů, kteří se spolupodílejí na jeho vytváření a jeho užíváním schvalují jeho obsah. Přestože výchozí formát a struktura mechanismu musí být někým navržena a vyvinuta, následné změny pravidel podléhají buďto většinovému či přímo celkovému konsensu. Lze zde tedy shledávat odraz tezí o společenské smlouvě, nikoliv však pasivně předvídané, ale aktivně uplatňované v rámci nastavení kyberprostorových pravidel daného blockchainu.

Vzhledem k výše naznačeným parametrům je pro další úvahy poměrně podstatné, že utváření legitimity skrze neustálé vytváření užšího či širšího koncensu nad podobou aktuální reality (tedy nejnovějšího bloku) či změnou v minulosti (tedy např. opravou záznamu v některém z bloků minulých) nevyhnutelně vede k nestálému větvení na více či méně důvěryhodné (a tím i životaschopné) paralelní řetězce záznamů. Mechanismus se tudíž odvrací od stanovení centrální autority definující legitimní realitu, a upřednostňuje přístup skrze množství alternativních realit, z nichž legitimní je ta, kterou si zvolí většina či všichni uživatelé jako podklad pro navazující jednání.[24]

Pravidla mechanismu konkrétního blockchainu jsou zabudována do jeho zdrojového kódu a matematické logiky, neplatí však, že jsou neměnná. Ke změně pravidel může dojít v podstatě bez omezení při vytváření nových bloků za předpokladu, že bloky s novými pravidly pro budoucí jednání převezme většina uživatelů. Nová pravidla přitom mohou mít podobu, která nekoliduje s dosavadním nastavením mechanismu (tzv. *soft fork,* např.

[23] Každý nový blok zpravidla obsahuje výsledek matematické *hash* funkce předchozího bloku, čímž jsou bloky postupně provázány do jednotného řetězce, ve kterém nemůže dojít k následné změně v minulých záznamech, aniž by to nezneplatnilo všechny následující bloky.

[24] Shodně viz SCLAVOUNIS, Odysseas. Understanding Public Blockchain Governance. *Oxford Internet Institute* [online]. 17. listopad 2017 [vid. 15. březen 2018]. Získáno z: https://www.oii.ox.ac.uk/blog/understanding-public-blockchain-governance/

přidání nových forem transakcí či dodatečných prvků a funkcí)[25] a pouze dočasně zdvojí aktuálně přípustné bloky, které se časem sjednotí, anebo dosavadní mechanismus naruší (tzv. *hard fork*), což vede k jeho rozvětvení na dva samostatné, které dále fungují paralelně podle odlišných pravidel, přičemž legitimními zůstávají oba za předpokladu, že je uživatelé neopustí.[26]

7. PARADOX DECENTRALIZOVANÉ SPRÁVY BLOCKCHAINU

Vlastní autorizace transakce či vytvoření nového záznamu v bloku je podmíněna specifickým procesem, který se převážně označuje jako těžba (*mining*).[27] Ten spočívá ve shromáždění záznamů z určitého časového úseku, vytvoření nového bloku s těmito záznamy, splnění požadavku daného blockchainu pro získání priority pro přidání tohoto bloku k blokům předchozím a následné distribuci nového bloku v rámci sítě. Ve vztahu k nalézání legitimity je z tohoto procesu nejzásadnější formulace pravidla pro stanovení příjemce priority pro přidání nového bloku. To může nabývat různých forem, převážná většina však vychází z oprávnění zdůvodněného vynaloženým úsilím (*proof of work*)[28] nebo relevantním podílem (*proof of stake*).[29]

Princip *proof of work* v zásadě odměňuje nárokem na přidání nového bloku toho z tvůrců bloků, který dokáže nejrychleji zašifrovat blok záznamů podle daných pravidel. V případě kryptoměny Bitcoin je pravidlem nalezení čísla, které při doplnění na konec bloku a zašifrování za pomoci SHA-256 bude začínat stanoveným počtem bitů s hodnotou 0. Jelikož generování šifrované *hash* funkce v dnešních možnostech nepodléhá předvídatelným matematickým pravidlům, může být dané doplňované číslo nale-

[25] Soft Fork. *Investopedia* [online]. [vid. 15. březen 2018]. Získáno z: https://www.investopedia.com/terms/s/soft-fork.asp

[26] Hard Fork. *Investopedia* [online]. [vid. 15. březen 2018]. Získáno z: https://www.investopedia.com/terms/h/hard-fork.asp

[27] Bitcoin Mining. *Investopedia* [online]. [vid. 15. březen 2018]. Získáno z: https://www.investopedia.com/terms/b/bitcoin-mining.asp

[28] Proof of Work. *Investopedia* [online]. [vid. 15. březen 2018]. Získáno z: https://www.investopedia.com/terms/p/proof-work.asp

[29] Proof of Stake. *Investopedia* [online]. [vid. 15. březen 2018]. Získáno z: https://www.investopedia.com/terms/p/proof-stake-pos.asp

zeno pouze za pomoci vysokého množství kalkulací, které náhodně doplňují různé hodnoty. Tím je zajištěno, že vytváření bloků je poměrně nesnadné a převážně náhodně distribuované mezi subjekty usilující o toto oprávnění. Výsledná náhodnost je také významným faktorem pro zvýšení důvěryhodnosti záznamů skrze pravidlo nejdelšího řetězce, jelikož nejdelší, tedy nejrychleji generovaný řetězec bloků se záznamy bude statisticky daleko pravděpodobněji ten, na jehož generování je vynaloženo největší celkové úsilí, a tedy se o jeho vytváření a další užití snaží nejvíce subjektů. Přestože tedy mechanismus připouští vytváření paralelních řetězců, zajišťuje, že dlouhodobě legitimním je pouze jeden a ostatní budou záhy opuštěny pro ekonomickou neúnosnost.

Jelikož výše zmíněný princip je vysoce neefektivní při porovnání celkového vynaloženého úsilí (soutěžící výpočetní kapacity) a dosaženého výsledku (přidání nového bloku),[30] sledují jiné adaptace blockchainu úspornější princip *proof of stake*. V tomto případě je tvůrce následujícího bloku volen v zásadě náhodně, případně náhodně za využití preferenčních faktorů, ve snaze o dosažení co nejširší distribuce oprávnění mezi subjekty zúčastněné na blockchainu. Problém, se kterým se tento systém potýká, jsou však nízké náklady spojené s alternativními řetězci,[31] tedy v podstatě alternativními realitami, a tudíž nižší krátkodobá důvěryhodnost záznamů a větší nejistota o celkové legitimitě. Ve snaze o odstranění těchto nedostatků jsou aplikovány různé modifikace či doplnění principu, ať už skrze částečnou kontrolu vývojáři blockchainu, kteří se tak stávají do jisté míry definiční autoritou,[32] nastavením limitů, které však daný problém pouze oddalují, nebo kombinací s jiným principem. Kromě částečného zapojení *pro-*

[30] Nejužívanější blockchain na této bázi, tedy původní blockchain pro kryptoměnu Bitcoin v současné době především z tohoto důvodu spotřebuje srovnatelné množství elektrické energie jako celé Maďarsko. Viz Bitcoin Energy Consumption Index. *Digiconomist* [online]. 2018 [vid. 15. březen 2018]. Získáno z: https://digiconomist.net/bitcoin-energy-consumption

[31] Problém je blíže popsán v ANDRUIMAN. PoS forging algorithms: multi-strategy forging and related security issues. *Scribd* [online]. 1. únor 2015 [vid. 15. březen 2018]. Získáno z: https://www.scribd.com/document/256072839/PoS-forging-algorithms-multi-strategy-forging-and-related-security-issues

[32] K tomuto přistoupili například vývojáři kryptoměny Peercoin. *peercoin* [online]. [vid. 15. březen 2018]. Získáno z: http://peercoin.net

of of work (např. koncept *proof of activity*[33]*)* je někdy využíváno obdobných pravidel vyžadujících vynaložení místa na disku (*proof of space* či *proof of capacity*) nebo vzdání se části hodnoty vytvářené v rámci blockchainu (*proof of burn*).

Problematické je, že v delším časovém rámci lze u mechanismu *proof of work* (ale též u dalších zmíněných principů) předpokládat koncentrační tendence. Rentabilita tvorby bloků je zde úzce spojena s investicemi do vysokého výpočetního výkonu a nízkými náklady na elektrickou energii pro maximalizaci pravděpodobnosti úspěšně vynaloženého úsilí.[34] S rostoucí náročností budou tedy ekonomické zákonitosti výnosů z rozsahu koncentrovat tuto funkci stále užší skupině, která bude mít nejrozsáhlejší investiční pozici v daném blockchainu.[35]

Pokud užijeme tohoto prizmatu k pohledu na vnitřní strukturu a fungování technologie blockchain, vystupuje na povrch skutečnost, na kterou upozorňoval již v roce 2016 pod výstižným označením „*blockchain paradox*" Vili Lehdonvirta v rámci své analýzy ohledně vhodného přístupu k regulaci blockchainu pro potřeby vlády Spojeného království,[36] tedy že přes zdánlivé technologické řešení vnitřní správy a organizace postavené na „nestranné logice kódu" nelze uniknout koncentraci vlivu a vytváření mocenských střetů ohledně nastavení definičních norem sítě. V tomto směru však blockchain nenabízí inovativní nástroj pro legitimaci této pravomoci ze strany

[33] Viz BENTOV, Iddo et al. *Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake* [online]. B.m.: International Association for Cryptologic Research. 2014 [vid. 15. březen 2018].

[34] Nelze se pak divit absurdním situacím, jako je ta v současné době se odehrávající na poli těžby kryptoměn v kolabující Venezuele. Viz ALTHAUSER, Joshua. Bitcoin Mining Thrives in Venezuela Thanks to Hyperinflation and Free Electricity. *Cointelegraph* [online]. 8. září 2017 [vid. 15. březen 2018]. Získáno z: https://cointelegraph.com/news/bitcoin-mining-thrives-in-venezuela-thanks-to-hyperinflation-and-free-electricity

[35] O rozsahu některých investic může vypovídat následující reportáž z industriálního přístupu k těžbě kryptoměny Bitcoin v Číně, kde je k tomu v jedné lokalitě využíváno více než 25 000 výpočetních zařízení. Viz WONG, Joon Ian; SIMON, Johny. Inside one of the world's largest bitcoin mines. *Quartz* [online]. 17. srpen 2017 [vid. 15. březen 2018]. Získáno z: https://qz.com/1055126/photos-china-has-one-of-worlds-largest-bitcoin-mines/

[36] LEHDONVIRTA, Vili. The blockchain paradox: Why distributed ledger technologies may do little to transform the economy. *Oxford Internet Institute* [online]. 21. listopad 2016 [vid. 15. březen 2018]. Získáno z: https://www.oii.ox.ac.uk/blog/the-blockchain-paradox-why-distributed-ledger-technologies-may-do-little-to-transform-the-economy/

definiční autority, pouze ji přenáší na vyšší a formálně neupravenou úroveň ekonomického střetu o právo silnějšího. Lze dokonce zvažovat, zda tato absence formalizované struktury pro transparentní dělbu moci v rámci správy blockchainu, tedy v rámci jeho decentralizované definiční autority, není v konečném důsledku méně legitimní, než v případě centralizované definiční autority vytvářené na základě tradičních organizačních struktur. Ve vztahu k vnímání blockchain jakožto vhodné adaptaci konceptu společenské smlouvy na pravidla kyberprostoru je však na místě uzavřít, že při podrobnějším zkoumání systém nenabízí skutečné řešení, ale pouze zdánlivou zástěrku transparentní aktivní participace většiny, která však ve skutečnosti skýtá tendence ke koncentraci autoritativního výkonu moci na základě míry investice a jiných faktorů, které vzbuzují pochybnosti o transparentní legitimitě této organizace definiční autority.

8. ZÁVĚR

Teorie společenské smlouvy jakožto základ pro přiznání legitimity výkonu autoritativní moci stojí u jádra struktury současné západní civilizace. Je zřejmé, že se tento koncept potýká s výzvami přicházejícími s proměnou společnosti vlivem technologického pokroku a zvláště pak v důsledku vytvoření kyberprostoru, ve kterém je v důsledku specifických vlastností tohoto prostředí na místě uvažovat o vhodném přizpůsobení tohoto legitimačního konceptu. V předchozím textu bylo stručně pojednáno o technologii blockchain a systému vytváření definičních norem a výkonu autoritativní moci v rámci této struktury. Při hlubším rozboru byl následně dovozen názor, že ačkoliv se blockchain mohl z teoretického hlediska zdát alternativním modelem pro zajištění legitimity definiční autority, při bližším pohledu je pravděpodobné, že jde pouze o novou technologii, která sice přenáší problém na novou úroveň, ale v jeho vlastní podstatě jej neřeší.

9. SEZNAM LITERATURY

[1] ALTHAUSER, Joshua. Bitcoin Mining Thrives in Venezuela Thanks to Hyperinflation and Free Electricity. *Cointelegraph* [online]. 2017. [vid. 15. březen 2018]. Získáno z: https://cointelegraph.com/news/bitcoin-mining-thrives-in-venezuela-thanks-to-hyperinflation-and-free-electricity

[2] ANDRUIMAN. PoS forging algorithms: multi-strategy forging and related security issues. *Scribd* [online]. 2015. [vid. 15. březen 2018]. Získáno z: https://www.scribd.com/document/256072839/PoS-forging-algorithms-multi-strategy-forging-and-related-security-issues

[3] ANTONOPOULOS, Nick; GILLAM, Lee. *Cloud Computing: Principles, Systems and Applications*. Londýn: Springer, 2017. ISBN 978-3-319-54645-2.

[4] BARLOW, John Perry. A Declaration of the Independence of Cyberspace. *Electronic Frontier Foundation* [online]. 1996. [vid. 15. březen 2018]. Získáno z: https://www.eff.org/cyberspace-independence

[5] BENTOV, Iddo et al. *Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake* [online]. 2014. B.m.: International Association for Cryptologic Research. [vid. 15. březen 2018]. Získáno z: http://eprint.iacr.org/2014/452

[6] CANEVARO, Mirko. *The Rule of Law as the Measure of Political Legitimacy in the Greek City States* [online]. 2017 [vid. 15. březen 2018]. Získáno z: https://link.springer.com/article/10.1007/s40803-017-0054-1

[7] HOBBES OF MALMESBURY, Thomas. *Leviathan* [online]. 1651 [vid. 15. březen 2018]. Získáno z: https://www.gutenberg.org/files/3207/3207-h/3207-h.htm

[8] HUSOVEC, Martin. *Zodpovednosť na internete podľa českého a slovenského práva* [online]. CZ.NIC. Praha: CZ.NIC, 2014 [vid. 24. srpen 2017]. ISBN 978-80-904248-8-3. Získáno z: https://knihy.nic.cz/files/edice/zodpovednost_na_internete.pdf

[9] CHERTOFF, Michael. A public policy perspective of the Dark Web. *Journal of Cyber Policy* [online]. 2017, roč. 2, č. 1, s. 26–38. ISSN 2373-8871. Získáno z: doi:10.1080/23738871.2017.1298643

[10] ICANN. Welcome to the global community! *icann.org* [online] [vid. 15. březen 2018]. Získáno z: https://www.icann.org/get-started

[11] KASL, František. European Smart Regulation of the Distributed Ledger Technology in the Financial Sector. In: SCHWEIGHOFER, Erich et al. (eds.) . *Trends and Communities of Legal Informatics IRIS 2017 Proceedings of the 20th International Legal Informatics Symposion*. Vídeň: Oesterreichische Computer Gesellschaft, 2017. ISBN 978-3-903035-15-7.

[12] LEHDONVIRTA, Vili. The blockchain paradox: Why distributed ledger technologies may do little to transform the economy. *Oxford Internet Institute* [online]. 2016. [vid. 15. březen 2018]. Získáno z: https://www.oii.ox.ac.uk/blog/the-blockchain-paradox-why-distributed-ledger-technologies-may-do-little-to-transform-the-economy/

[13] LESSIG, Lawrence. *Code and Other Laws of Cyberspace*. New York: Basic Books, 1999, 297 s. ISBN 0-465-03912-X.

[14] LESSIG, Lawrence. *Code: Version 2.0*. New York: Basic Books, 2006, 410 s. ISBN 978-0-465-03914-2.

[15] LOCKE, John. *Druhé pojednání o vládě*. Přel. KRÁL, Josef. Praha: Svoboda, 1992, 184 s. ISBN 80-205-0222-X.

[16] NOZICK, Robert. *Anarchy, State, and Utopia*. New York: Basic Books, 1974, 334 s. ISBN 0-465-09720-0.

[17] PASTOR-SATORRAS, Romualdo; VESPIGNANI, Alessandro. *Evolution and Structure of the Internet: A Statistical Physics Approach*. Cambridge: Cambridge University Press, 2007. ISBN 978-0-521-82698-3.

[18] POLČÁK, Radim. *Internet a proměny práva*. Praha: Auditorium, 2012. ISBN 978-80-87284-22-3.

[19] RAWLS, John. *A Theory of Justice*. Cambridge, Massachusetts: Belknap Press of Harvard University Press, 1971, 560 s. ISBN 0-674-00078-1.

[20] ROUSSEAU, Jean-Jacques. *O společenské smlouvě neboli zásadách státního práva*. Plzeň: Aleš Čeněk, 2002, 157 s. ISBN 80-86473-10-4.

[21] SATOSHI NAKAMOTO. *Bitcoin: A Peer-to-Peer Electronic Cash System* [online]. 2008. B.m.: www.bitcoin.org. [vid. 15. březen 2018]. Získáno z: https://bitcoin.org/bitcoin.pdf

[22] SCLAVOUNIS, Odysseas. Understanding Public Blockchain Governance. *Oxford Internet Institute* [online]. 2017. [vid. 15. březen 2018]. Získáno z: https://www.oii.ox.ac.uk/blog/understanding-public-blockchain-governance/

[23] TAMANAHA, Brian Z. *On the Rule of Law: History, Politics, Theory*. Cambridge: Cambridge University Press, 2004. ISBN 521-84362-6.

[24] WONG, Joon Ian; SIMON, Johny. Inside one of the world's largest bitcoin mines. *Quartz* [online]. 2017. [vid. 15. březen 2018]. Získáno z: https://qz.com/1055126/photos-china-has-one-of-worlds-largest-bitcoin-mines/

[25] The great chain of being sure about things. *The Economist* [online]. 2015 [vid. 15. březen 2018]. ISSN 0013-0613. Získáno z: https://www.economist.com/news/briefing/21677228-technology-behind-bitcoin-lets-people-who-do-not-know-or-trust-each-other-build-dependable

[26] Bitcoin Energy Consumption Index. *Digiconomist* [online]. 2018. [vid. 15. březen 2018]. Získáno z: https://digiconomist.net/bitcoin-energy-consumption

[27] Bitcoin Mining. *Investopedia* [online]. [vid. 15. březen 2018]. Získáno z: https://www.investopedia.com/terms/b/bitcoin-mining.asp

[28] Hard Fork. *Investopedia* [online]. [vid. 15. březen 2018]. Získáno z: https://www.investopedia.com/terms/h/hard-fork.asp

[29] Peercoin. *peercoin* [online] [vid. 15. březen 2018]. Získáno z: http://peercoin.net

[30] Proof of Stake. *Investopedia* [online]. [vid. 15. březen 2018]. Získáno z: https://www.investopedia.com/terms/p/proof-stake-pos.asp

[31] Proof of Work. *Investopedia* [online]. [vid. 15. březen 2018]. Získáno z: https://www.investopedia.com/terms/p/proof-work.asp

[32] Soft Fork. *Investopedia* [online]. [vid. 15. březen 2018]. Získáno z: https://www.investopedia.com/terms/s/soft-fork.asp