ZLOUPORABE *BLOCKCHAIN* TEHNOLOGIJE I UTJECAJ NA TRGOVAČKA DRUŠTVA

*Prof. dr. sc. Edita Čulinović-Herc**

UDK 347.72:004.3/.4]:17
https://doi.org/10.30925/zpfsr.43.3.9
Ur.: 31. ožujka 2022.
Pr.: 8. svibnja 2022.
Prethodno priopćenje

Sažetak

Blockchain *tehnologija koja se svrstava u tehnologije distribuiranog knjiženja ima široku primjenu u poslovanju trgovačkog društva. Znatno je podnormirana, izmiče regulatornom nadzoru i podložna je zlouporabama. U radu se analiziraju neki pojavni oblici zlouporaba BC tehnologije, rizici koji su nastupili kao i pitanje kome se može, od sudionika pripisati u odgovornost napad na sustav. Također se rizici primjene DLT/BC tehnologije sagledavaju iz kuta trgovačkoga društva, kao naručitelja novih tehnoloških rješenja te se traži odgovor na pitanje tko bi u trgovačkom društvu trebao brinuti o primjeni novih tehnoloških rješenja i prevenirati nastupe tih rizika.*

Ključne riječi: blockchain *tehnologija; zlouporabe BC tehnologije; trgovačka društva; odgovornost ključnih razvojnih programera.*

1. UVOD – TRGOVAČKA DRUŠTAVA U DIGITALNOM OKRUŽJU

Trgovačka društva primjenjuju razne digitalne alate utemeljene na tehnologiji distribuiranog knjiženja (dalje: DTL) i pri nuđenju proizvoda i usluga i u korporativnom upravljanju društvom. U tu grupu tehnoloških rješenja pripada i *blockchain* tehnologija (dalje: BC), koji je pojavni oblik DLT-a.[1] S njihovom primjenom povezani su i pametni ugovori.[2] Mogućnosti su primjene BC tehnologije brojne: od protokoliranja, evidentiranja i pohranjivanja podataka o korporativnim događajima[3] do digitalizacije

* Dr. sc. Edita Čulinović-Herc, redovita profesorica u trajnom zvanju, Sveučilište u Rijeci, Pravni fakultet; edita@pravri.hr. ORCID ID: orcid.org/0000-0002-6177-8057.
Ovaj rad financiralo je Sveučilište u Rijeci projektom *Pravni aspekti restrukturiranja trgovačkih društava i tranzicija prema novoj kulturi korporativnog upravljanja* (uniridrustv-18-43).

1 Primavera de Filippi i Aaron Wright, *Blockchain and the Law - The Rule of Code* (Cambridge, Mass: Harvard University Press, 2018.), 1-250, Dirk A. Zetzsche, Ross P. Buckley i D.W. Arner, „The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain", *University of Illinois Law Review* br. 4 (2018): 1382-1402.

2 Philip Trillmich, Matthias Goetz i Chris Ewing; „Blockchain and Smart Contracts", u: *Handbook of Blockchain law,* ed. Matthias Artzt, Thomas Richter (The Hague: Wolters Kluwer, 2020.), 163-192.

3 Vidi primjere u Luca Enriques i Dirk A. Zetzsche, „Corporate Technologies and the Tech Nirvana

važnih poslovnih operacija (engl. *supply chain management*). Također je čitav niz sofverskih rješenja utemeljenih na BC tehnologiji za praćenje raznih poslovnih funkcija u društvu *(*engl. *governance, risk and compliance)*.[4]

Primjena novih tehnologija ujedno i mijenja trgovačko društvo, posebice u organizacijskom smislu i smanjuju potrebu za ljudskim radom.[5] Korporativni giganti prolaze kroz transformaciju, usitnjavajući se na manja trgovačka društva koja, s jedne strane, koriste prednosti što su članovi poslovnoga konglomerata, a s druge, kao manji entiteti lakše se nose s izazovom inovativnosti.[6] S druge strane, svjedočimo brzom, katkad strelovitom rastu, osobito tehnoloških, startupova.[7]

No, što je uopće BC tehnologija? Riječ je o tehnologiji distribuiranog knjiženja. To znači da se podatci knjiže simultano na svim računalima u mreži, a ne na jednom, središnjem mjestu. Načelno, valjanost novih transakcija ili autoriziranoga prijenosa podataka, neovisno o području u kojoj se koristi, ne odobrava jedna središnja točka, poput središnjeg registra (engl. *central ledger*), već sami sudionici mreže, primjenom metode konsenzusa (engl. *consensus protocol*). (Nakon odobrenja, transakcije se zapisuju kao novo promijenjeno stanje podataka na BC-u, a koje je kao takvo vidljivo sudionicima mreže. Mreža može biti javna, bez nadzora ulaska i privatna ili poluprivatna s ograničenim ulaskom. Svi protokoli postupanja s podatcima i transakcijama kodirani su algoritmom. Ističe se da zbog čvrstoga kodiranja nije niti potrebno imati povjerenje u drugu ugovornu stranu, odnosno u posrednika.[8] Tim konceptom decentralizacije u knjiženju i nepostojanja kontrole središnjega tijela[9] teži se zaobići tradicionalne posrednike, ali i regulatore.

No, ako nešto u primjeni BC tehnologije pođe po zlu, potrebna je ljudska akcija. Iako se zagovara načelo netokracije, na odluku o načinu oporavka BC sustava, posebice ako je oporavak posljedica napada, utječu ključni razvojni programeri (engl. *core developers*). Kodiranje ima svojih nedostataka. Namjerne ili slučajne pogreške u programiranju često su uzrok hakerskih napada. Napadi na BC sustav i nedostatci u programiranju otvaraju pitanje odgovornosti. U doktrini SAD-a vodi se žestoka rasprava trebaju li ključni razvojni programeri ponijeti teret odgovornosti na temelju fiducijarnih dužnosti. Postoje i zagovaratelji i protivnici toga koncepta.[10]

Fallacy", *ECGI, Law Working Paper* br. 457 (2019): 13-15, https://ssrn.com/abstract=3392321.

4 Kenneth Bamberger, „Technologies of Compliance: Risk and Regulation in a Digital Age", *Texas Law Review* 88, br. 4 (2010): 674.

5 Mark Fenwick i Erik P. M. Vermeulen, „The New Firm: Staying Relevant, Unique and Competitive", *European Business Organization Law Review* 16, br. 4 (2015): 599.

6 Fenwick *et al.*, *The New Firm*, 606.

7 *OECD Studies on SMEs and Entrepreneurship Understanding Firm Growth Helping SMEs Scale Up* (Paris: OECD, 2021.), 59-75.

8 Esther Shein, „How Blockchain Changes the Nature of Trust", https://linuxfoundation.org/blog/how-blockchain-changes-the-nature-of-trust/.

9 Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System, 2008.,* https://bitcoin.org/en/bitcoin-paper, 1-9.

10 Zagovornik ideje je Angela Walch, „In Code(rs) we trust: Software developers as fiduciaries in public blockchains", u: *Regulating Blockchain: Techno-Social and Legal Challenges*, Philipp Hacker, Ioannis Lianos, Georgios Dimitropoulos i Stefan Eich (Oxford: Oxford Scholarship online, 2019.), 59-75. Protivnici su Raina S. Haque, Rodrigo Seira Silva-Herzog, Brent A.

Zakonodavci, akademski stručnjaci, pravnici i inženjeri bore se, svako u svom području, s regulatornim i etičkim izazovima primjene tehnologija utemeljene na DLT/BC-u.[11]

BC tehnologije su i općenito podijelile akademsku javnost. Tehnološki optimisti vjeruju u supremaciju tehnologije nad pravom, do te mjere da smatraju da pravo nije više niti potrebno, jer se sve što je potrebno nalazi u algoritamskom kodu.[12] Tehnološki realisti ili skeptici tvrde da će nove tehnologije u trgovačkom društvu svakako riješiti neka stara pitanja sukoba interesa koja izviru iz problema „odjeljivanja vlasništva od kontrole" (engl. *agency problem*), ali da će generirati i nove. [13] Tako se navodi da osoba koja kontrolira dizajn novoga tehnološkog rješenja neizravno nadzire i samu tehnologiju.[14] Stoga se postavlja se pitanje, tko bi u trgovačkom društvu trebao voditi brigu o odabiru BC-rješenja, a da se u društvu ne pogoduje niti jednoj interesnoj skupini, čiji bi interesi mogli odnijeti prevagu nad interesima društva.

Zadatak je ovog rada upozoriti na pitanja zlouporaba BC tehnologije, otvoriti raspravu o pitanju odgovornosti ključnih razvojnih programera te povezati primjenu BC tehnologije s trgovačkim društvima kao njihovim korisnicima. Stoga se u nastavku rada iznose dva primjera zlouporaba nastalih kao posljedica hakerskoga napada na BC sustav te se iznose pristupi prepoznavanja odgovornih osoba, kao i osnova te odgovornosti, s obzirom na posebnosti BC tehnologije i nepostojanje posebnih propisa. U nastavku, s obzirom na to da će glavni naručitelji BC rješenja biti gospodarski veća i snažnija društva, poput dioničkih društava, istražuje se tko bi u trgovačkom društvu trebao brinuti o odabiru i osiguranju primjene kvalitetne i nepristrane BC tehnologije.

2. ZLOUPORABE BC TEHNOLOGIJE, PREPOZNATI RIZICI I ODGOVORNOST

Povijest trgovačkih društava ujedno je povijest korporativnih skandala, koji su pokretači zakonodavnih promjena. Česti napadi na BC platforme pogotovo one na kojima se trguje kriptovalutama dodatno upozoravaju na potrebu regulatorne akcije. Riječ je o zlouporabama sustava napadom izvana, zbog kojih je došlo zbog praznina/nedostataka u algoritamskom kodu, primijenjene potpuno različite metode oporavka, pod utjecajem ključnih razvojnih programera. To stvara stanje visoke pravne (ne) sigurnosti, ne samo za korisnike usluga koje nudi BC mreža, nego i za sudionike koji imaju proaktivniju ulogu.

Plummer i Nelson M. Rosario, „Blockchain Development and Fiduciary Duty" *Stanford Journal of Blockchain Law & Policy* 2, (2019): 139-187.

11 Michele B. Neitz, „The Influencers: Facebook's Libra, Public Blockchains, And the Ethical Considerations of Centralization", *North Carolina Journal of Law & Technology* 21, br. 2 (2019): 18.

12 De Filippi *et al.*, *Blockchain and the Law*, 5-9.

13 Enriques *et al.*, *Corporate Technologies*, 8.

14 Enriques *et al.*, *Corporate Technologies*, 49.

2.1. Napad na DAO i primjena „tvrde vilice“

Decetralizirana autonomna organizacija (DAO) skup je pametnih ugovora[15] na BC mreži *Ethereum*, na kojoj se trguje kriptovalutom pod nazivom *ether*. Pametni ugovori (engl. *smart contracts*) računalni su protokoli koji izvršavaju, nadziru i/ili dokumentiraju pravno relevantne radnje (posebice izvršenje ugovornih obveza) uvjetujući ih digitalno utvrdljivim rezultatima.[16] Pametni se ugovor razlikuje od klasičnoga po svojoj samoispunjivosti,[17] odnosno obveze se ispunjavaju s malo ili bez ljudske aktivnosti. Njihov je koncept sazdao odvjetnik i kriptograf Nick Szabo 1994. te ih je opisao kao kompjutorizirane transakcijske protokole koji izvršavaju uvjete ugovora.[18] To su skupovi kodova koji određuju uvjete pod kojima će se određene računalne operacije izvršiti, a kao rezultat njihova izvršenja dolazi do slanja ili premještanja podataka.[19] Neizmjenjivost, odnosno nezaustavljivost pametnih ugovora ujedno je njihova prednost i nedostatak.

DAO o kojem je riječ, osnovan je 2016. kako bi se omogućilo financiranje *startup* projekata u zajedničkoj virtualnoj organizaciji.[20] Jentzsch, teorijski fizičar, došao je na ideju da se skupno financiranje za *startupove* ne provodi za svaki novi zasebno, već putem ulaganja u DAO (engl. *Decentralized Autonomous Organization*). DAO je bio taj koji je ta sredstva ulagao u *startupove* ili projekte odabirom imatelja tokena u DAO-u, odnosno svojih članova. Tijekom inicijalne ponude tokena DAO-a u svibnju 2016., prikupljeno je virtualne valute u vrijednosti oko 150 milijuna USD, čime je oboren rekord u sredstvima koja su prikupljena skupnim financiranjem.

Međutim, 16. lipnja 2016. došlo je do napada na DAO zbog postojanja određenih nedostataka u njegovu kodu.[21]

Naime, kod je imao programiranu, tzv. zaštitu manjine. Imatelji tokena koji bi glasali protiv nekoga projekta kojeg je većina prihvatila mogli su inicirati podjelu DAO-a. Manjina je mogla svoje tokene / *ethere* prenijeti u novi DAO (dalje: *DAO child*) koji je bivao podvrgnut istim pravilima kao i inicijalni DAO.[22] No, protokol podjele bio je čvrsto kodiran. Prijedlog za podjelu morao je biti najmanje tjedan dana u raspravi. Nakon toga, funkcija podjele mogla se aktivirati, a tokeni inicijatora

15 Neitz, *The Influencers*, 10.

16 Kaulartz, Markus i Jörn Heckmann, „Smart Contracts – Anwendungen der Blockchain-Technologie“, *Computer und Recht* 32, br. 9 (2016): 618-624.

17 O četiri etape pametnih ugovora vidi Nathan Tse, „Decentralised Autonomous Organisations and the Corporate Form“, *Victoria University of Wellington Law Review* 51, br. 3 (2020): 319.

18 Nick Szabo, *Smart contracts* (1994), https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html.

19 Trillmich et al., *Blockchain and Smart Contracts*, 165.

20 Antonio Garcia Rolo, „Challenges in the Legal Qualification of Decentralised Autonomous Organisations (DAOs): The Rise of the Crypto-Partnership?“, *Revista de Direito e Tecnologia* 1, br. 1 (2019): 33-87.

21 David Siegel, *Understanding The DAO Attack*, https://www.coindesk.com/learn/2016/06/25/understanding-the-dao-attack/

22 Lefteris Karapetsas, *How to split the DAO* (2016), https://github.com/slockit/DAO/wiki/How-to-split-the-DAO

podjele mogli su se prenijeti u *DAO child*. No nakon toga slijedilo je razdoblje od 27 dana tijekom kojeg je bilo zabranjeno iznositi ikakav prijedlog. Nakon isteka tog roka, mogao se je podnijeti prijedlog za prijenos *ethera* (na temelju pripadajućih tokena) iz *DAO child* na vlastiti račun, ali ne prije isteka dodatnoga roka od 14 dana. Drugim riječima, nakon što bi započeo postupak podjele DAO-a, bilo je potrebno najmanje 48 dana da virtualna valuta „sjedne na račun" inicijatora podjele.[23]

Napadač je iskoristio nedostatke u kodiranju protokola. Nakon aktivacije funkcije podjele DAO-a, kôd bi prvo označio tokene / *ethere*, koji će prijeći u *DAO child*, no nije istodobno ažurirao stanje na računu inicijalnog aDAO-a. K tome, kôd nije zaštitio protokol podjele od, tzv. rekurzivnog poziva. To je izraz koji se koristi za označavanje funkcije „koja poziva samu sebe". Napadač je uspio „rekurzivno pozvati" funkciju podjele i dohvatiti sredstva više puta prije nego što je hodogram podjele došao u onu točku u kojoj kôd sam provjerava stanje *ethera* na računu DAO-a.

Napadač je zloupotrebom rekurzivnog poziva, 16. lipnja 2016. uspio iz DAO-a prisvojiti oko 3,6 milijuna ethera, što je iznosilo otprilike trećinu sredstava cijelog DAO-a. Nakon objave događaja, vrijednost *ethera* se gotovo prepolovila.[24] Dakle, dva su čimbenika omogućila napad. Kod nije bio zaštićen od rekurzivnoga poziva, a pametni ugovor nije bio tako programiran da bi istodobno sa slanjem valute ažurirao saldo. U bitnome riječ je o nedostatcima u kodiranju.[25]

Uslijedila je intenzivna rasprava u BC zajednici što je potrebno učiniti. Napadač je objavio otvoreno pismo ethereum zajednici,[26] u kojem je tvrdio da prisvajanje sredstava nije bilo nezakonito jer da je kôd zakon. Smatrao je da nije legitimno njegovu transakciju smatrati nevaljanom jer je sve stečeno upravo prema uvjetima pametnog ugovora. Zbog gore objašnjenog protokola podjele, BC zajednica imala je na raspolaganju 27 dana da donese odluku o načinu oporavka sustava od napada prije negoli napadač pokrene prijedlog za prijenos ethera na svoj račun.[27]

Zajednica je razmatrala primjenu, tzv. „meke ili tvrde vilice", kao i to treba li uopće išta poduzeti. „Meka vilica" (engl. *soft fork*) značila bi da sve (buduće) transakcije, kojima bi se povukla sredstva iz DAO-a smatrale nevaljanima. Transakcije koje su se odvile do primjene „meke vilice" bile bi valjane. „Tvrda vilica" (engl. *hard fork*) prebrisala bi povijest svih transakcija DAO-a od početka obavljanja djelatnosti. Oponenti tih dvaju rješenja oslanjali su se na filozofske temelje *ethereum blockchaina*. Tvrdili su, kao i napadač, da je „kôd zakon" i da je sve što dopušta kôd - legitimno. Primjena „tvrde vilice" ugrožavala je načelo nepromjenjivosti zapisa kao jednu od najvažnijih odlika BC-a. Ključni razvojni programeri predložili su najprije „meku

23 Osman Gazi Güçlütürk, *The DAO Hack Explained: Unfortunate Take-off of Smart Contracts*, https://ogucluturk.medium.com/the-dao-hack-explained-unfortunate-take-off-of-smart-contracts-2bd8c8db3562

24 David Hirsch, „Blockchain and Information Security", u: *Handbook of Blockchain law*, ed. Matthias Artzt; Thomas Richter (The Hague: Wolters Kluwer, 2020.), 117.

25 Zetzsche *et al.*, *The Distributed Liability*, 1381.

26 Pismo napadača, v. DAO Hack, Attacker Sends Open Letter to Ethereum Community, 23.09.2022. https://www.newsbtc.com/news/dao-hack-attacker-sends-open-letter-to-ethereum-community/

27 Güçlütürk, *DAO Hack Explained.*

vilicu".[28]

Glasovanje o „mekoj vilici" započelo je 22. lipnja 2016. Odluka je donesena većinom i trebala je biti provedena 30. lipnja 2016. Međutim, zbog dodatnih sigurnosnih nedostataka od „meke vilice" se putem odustalo.[29] Nakon toga krenula je rasprava o „tvrdoj vilici". Tvrdilo se da je napad bio preozbiljan da bi ga se moglo zanemariti. Odluku o primjeni „tvrde vilice" izglasala je i prihvatila većina rudara (engl. *miners*) *ethereum* zajednice.[30] „Tvrda vilica" dovršena je 20. srpnja 2016., a sredstva su vraćena ulagateljima.[31] Prema nekim autorima tu je odluku nametnulo sedam ključnih razvojnih programera.[32] Time je oblikovana i nova inačica mreže *Ethernum*, s drugim pravilima od izvornih. Nakon toga su rudari i drugi dionici mreže odlučivali žele li biti dionici nove verzije *Ethereuma* ili izvorne.[33] Izvorna inačica *Ethereuma* nastavila je djelovati kao *Ethereum Classic*.[34]

Iz ovog je primjera vidljivo da je BC zajednica odstupila od temeljnih tehnoloških postavki BC (kôd = zakon). Odluka je donesena pod utjecajem ključnih programera. S druge strane, odluke koje su jednom izglasane, u provedbi su napuštene („meka vilica"), što pokazuje i ozbiljne nedostatke u sustavu upravljanja i načinu donošenja odluka u BC zajednici. Ovaj je događaj svakako pobudio opću sumnju u BC tehnologiju i potaknuo raspravu o potrebi regulacije. Ljudska se prosudba pokazala nezamjenjivom, iako su svi problemi trebali biti previđeni i riješeni u pametnim ugovorima.

2.2. Napad na Parity *i neprimjena „tvrde vilice"*

Parity je trgovačko društvo koje je utemeljio Gawin Wood (inače suosnivač *Ethereuma*) s još nekim razvojnim programerima. Wood je bio i autor programa *Solidity* za programiranje pametnih ugovora. *Parity* je razvio koncept novčanika s više potpisa (engl. *multi-sig wallet*).[35] Osobitost je toga novčanika da se pri provedbi transakcije, zahtijeva primjena dvaju ili više privatnih ključeva, kako bi se sigurnije odobrila.

Parityju se nehotice potkrala pogreška u pametnim ugovorima, koja je omogućila da jedan korisnik jednostrano izmijeni imena vlasnika i parametre korištenja tuđih novčanika koji su sadržavali 150 tisuća *ethera*.[36] To je napadaču omogućilo da učini

28 Güçlütürk, *DAO Hack Explained.*
29 Andreas M. Antonopoulos i Gavin Wood, *Mastering Ethereum: building smart contracts and DApps* (Cambridge: O'Reilly, 2018.), 327.
30 Antonio Madeira, *The Dao, the Hack, the Soft Fork and the Hard Fork*, https://www.cryptocompare.com/coins/guides/the-dao-the-hack-the-soft-fork-and-the-hard-fork/
31 Michael del Castillo, *Ethereum Executes Blockchain Hard Fork to Return DAO Funds*, https://www.coindesk.com/tech/2016/07/20/ethereum-executes-blockchain-hard-fork-to-return-dao-funds/
32 Neitz, *The Influencers*, 10.
33 Matthew Leising, *The Ether Thief*, https://www.bloomberg.com/features/2017-the-ether-thief/.
34 Hirsch, *Blockchain and Information Security*, 118.
35 Hirsch, *Blockchain and Information Security*, 113.
36 Parity Technologies, *The Multi-sig Hack: A Postmortem*, https://www.parity.io/blog/the-multi-sig-hack-a-postmortem.

sebe vlasnikom triju novčanika te da prenese sredstva iz tih novčanika na novčanike koji su bili pod njegovom kontrolom. U otprilike isto vrijeme kada se to dogodilo, grupa hakera bijelog šešira (engl. *white hat hackers*) iskoristila je također taj nedostatak i prenijela na sebe sredstva idućih 593 novčanika, na kojima je bilo više od 377 tisuća *ethera*. Nakon što je *Parity* otklonio problem, sredstva su preknjižena na prave novčanike.

No u otklanjanju toga problema učinjena je još veća pogreška. Primijećeno je da novi, poboljšani pametni ugovor nije aktiviran, pa je dan nalog da se to učini. Pri njegovoj aktivacii novak, zaposlen u *Ethereum Foundation*, najprije je učinio sebe vlasnikom cijele knjižnice (engl. *library*) pametnih ugovora. Kontrola knjižnice pametnih ugovora značila je i kontrolu nad svim *multi-sig* novčanicima. S aktivacijom novoga programa došlo je do zamrzavanja sredstava na 584 novčanika u vrijednosti od oko 500 tisuća *ethera*.

Kako bi se novčanici vratili pravim vlasnicima, opet je trebalo primijeniti „tvrdu vilicu", za što su se zalagali oštećeni vlasnici novčanika. Međutim tomu su se usprotivili ključni razvojni programeri, pa je stanje na njima ostalo trajno zamrznuto. Kada je osnivač *Ethereuma*, Vitalik Buterin, upitan zbog čega je u slučaju napada na DAO primijenjena „tvrda vilica", a u ovom slučaju nije, odgovorio je da je tada sustav bio manje zreo i da je bio ugrožen proporcionalno veći iznos *ethera* te da u novim uvjetima napadač može povući sredstva, bez odgode, za razliku od DAO-a, tako da provedba „tvrde vilice" nije bila niti moguća.[37]

2.3. Prepoznati rizici, pravna kvalifikacija i odgovornost

2.3.1. Prepoznati rizici

Primjena „tvrde vilice" u slučaju napada na DAO i nedostatak njezine primjene u slučaju *Parity* upućuju na utjecaj ključnih razvojnih programera na BC sustav, jer su u sličnim situacijama napada, pod njihovim utjecajem donesene različite odluke. To otvara dvojbu. Jesu li ključni razvojni programeri u prvom slučaju bili pristrani i zaštitili ulagatelje „od svog povjerenja" ili su možda inzistirali na primjeni „tvrde vilice" jer su i sami bili pogođeni tim napadom? Kako se primjena „tvrde vilice" miri s jednim od temeljnih načela na kojima počiva BC tehnologija, a to je trajnost i nepromjenjivost zapisa?

I proces donošenja odluka bio je deficitan, pa su neki autori iz toga izveli zaključak da znatan dio procesa odlučivanja nije izrijekom uređen i da korisnici nisu u potpunosti osnaženi.[38] To se opet kosi s idejom „participativne demokracije jednakih" koju zagovara BC. Neki autori tvrde da je i način glasovanja bio postavljen tako da se omogući provedba „tvrde vilice".[39] S obzirom na to da je riječ o javnom BC-u,

37 Pismo Vitalika Buterina od 19. 7. 2021., https://twitter.com/VitalikButerin/status/887783867129745412.

38 Nick Tomaino, *The Governance of Blockchains*, https://thecontrol.co/the-governance-of-blockchains-5ba17a4f5da6

39 Trebalo je odgovoriti na pitanje „Jeste li protiv tvrde vilice?", odnosno pitanje je bilo postavljeno tako da se trebalo izjasniti protiv. Haque *et al.*, *Blockchain Development,* 170.

pojavila se zabrinutost da javnim BC-om upravlja mali broj ključnih osoba, koje zbog veličine svoga utjecaja mogu zagovarati odluke koje će odgovarati njihovim osobnim interesima, odnosno interesima skupina kojima pripadaju.[40]

U oba je primjera bilo riječ događaju (napad na sustav zbog nedostatka u kodiranju) koji se svrstava u operativne rizike. Nedostatak se nalazi na aplikaciji/protokolu koja je programirana na tom BC-u, a ne na samom BC-u. No, bitno je naglasiti da on u sustavu decentraliziranog knjiženja pogađa veći broj točaka, negoli kada postoji jedna središnja točka.[41] Kako ne postoji besprijekoran program, štoviše on se po putu unaprijeđuje, nedostatci u kodu su veliki operativan problem, jer upravo to otvara vrata hakiranju sustava.[42] No, u ovim primjerima prepoznat je i rizik koji se naziva rizik ključnih osoba (engl. *key person risk*). Malo je stručnjaka koji uopće razumiju kako funkcionira BC sustav, a još manje ih je u stanju popraviti pogreške u kodu kada se one otkriju. To posebno vrijedi za poluzatvorene BC sustave koji se temelje na dozvoli pristupa i gdje mala skupina ključnih programera ima pristup algoritamskom kodu. Oni pregledavaju i ocjenjuju prijedloge drugih programera, uključuju ono što smatraju dobrim prijedlozima i objavljuju revidirane verzije koda podobne za mrežno usvajanje. Manje promjene odobravaju naredbom, ali za veće se moderira javna rasprava o korisnosti promjene.[43] No, koliko god labava bila veza u virtualnoj organizaciji, ključni ljudi organizacije uvijek su rizik za organizaciju, jer se mogu razboljeti, biti korumpirani ili ucijenjeni.[44] Stoga se postavlja pitanje tko je odgovoran za nedostatnu uspješnost ili nedolično ponašanje ključnih osoba, osobito ako su to osobe koje utječu na druge korisnike BC mreže.[45]

2.3.2. Pravna kvalifikacija i odgovornost

Pri razmatranju pitanja odgovornosti u DLT/BC mrežama nužno je imati na umu osobitosti te tehnologije. Riječ je o participativnom i distribuiranom načinu knjiženja, pa prema tome i odvijanju transakcija. Zbog toga treba prvo krenuti od toga koje grupe sudionika uopće u sustavu postoje. U doktrini se uobičajeno prepoznaje pet različitih grupa sudionika DLT/BC mreže.[46] Kao prvo, ključna grupa razvojnih programera (engl. *core group*) dizajnira kod i *de facto* upravlja DLT/BC sustavom. Drugu grupu čine vlasnici dodatnih poslužitelja koji sudjeluju u validaciji transakcija (engl. *owners of additional servers for validation purposes*). Treću grupu čine kvalificirani korisnici (engl. *qualified users)* distribuirane knjige, kao što su primjerice kreditne institucije ili rudari (engl. *miners*). Jednostavni korisnici sustava (engl. *simple*

40 Kevin Werbach, „Trust, but Verify: Why Blockchain Needs the Law“, *Berkeley Technology Law Journal* 33, br. 2 (2018): 528-529.

41 Angela Walch, „The Bitcoin Blockchain as Financial Market Infrastructure: A Consideration of Operational Risk“, *New York University Journal of Legislation & Public Policy* 18, br. 4 (2015): 859-865.

42 Jake van der Laan, „Understanding Blockchain“, u: *Handbook of Blockchain law*, ed. Matthias Artzt, Thomas Richter (The Hague: Wolters Kluwer, 2020.), 45.

43 Zetzsche *et al*., *The Distributed Liability*, 1382.

44 Walch, *The Bitcoin Blockchain*, 860-861.

45 Zetzsche *et al.*, *The Distributed Liability*, 1382.

46 Zetzsche *et al.*, *The Distributed Liability*, 1384.

users) četvrta su grupa sudionika. To su, primjerice mali ulagači u virtualne valute. Postoje i treće strane (engl. *third parties*) na koje BC sustav utječe i bez da ga izravno koriste, na primjer, banke koje daju kredite jednostavnim korisnicima i sl.

Kada se DLT/BC proučava iz perspektive odgovornosti, s obzirom na brojne inačice njegova ustroja, prema Zetscheu i drugima, ključno je uzeti u obzir nekoliko pitanja.[47] Ponajprije nužno je odrediti upravljačku strukturu i uključene subjekte. Zatim je potrebno pojasniti koji se pravni standardi primjenjuju na koje DLT/BC procese i usluge. Tehnološki procesi moraju biti robusni što znači da treba posvetiti pojačanu pažnju poslužiteljskoj infrastrukturi, tko ima pravo pristupa i sl. Jedno od pitanja na koje se mora odgovoriti svakako je ono tko snosi odgovornost za integritet sustava, odnosno za pogreške u algoritmu.

Najteže je i ujedno najzanimljivije pitanje kako pravno kvalificirati suradnju između sudionika DLT/BC sustava.[48] U DLT/BC sustavu, svi su čvorovi izravno povezani, međusobno surađuju te metodom mrežnoga konsenzusa određuju koji će podatci biti pohranjeni u distribuiranoj knjizi, a koji ne. Riječ je o mreži ravnopravnih subjekata (engl. *peer-to-peer*). Veze s drugim čvorovima su istorazinske i stvarne, zbog veza među računalima. Izravna veza između računala je ono zbog čega, prema Zetzscheu i drugima mreža postaje i pravno povezana.[49] Mrežni konsenzus također je specifično obilježje, zbog kojeg se DLT/BC mreža opisuje kao sustav kontrole utemeljene na participaciji. Transakcija biva odobrena ako ju potvrdi 51 % čvorova u mreži ili toliko čvorova koji raspolažu s 51 % računalne snage. Bayern sugerira da je u BC sustavima nemoguće govoriti o ugovornim odnosima općenito - jer je korisnik nepoznat, korisnička baza nestabilna, a izvršenje usluge ovisi o tome tko je u koje vrijeme na mreži, a da pritom niti jedan od čvorova nije ključan.[50] No, ipak se postavlja pitanje je li radnja preuzimanja besplatnog softvera od novoga korisnika ujedno i prihvat ponude za sudjelovanje u obavljanju usluge distribuiranoga knjiženja. No, ako postoje problemi uspostave ugovorne veze, tada se pravni konstrukt odgovornosti mora graditi na izvanugovornoj, što može biti osobito važno za odgovornost ključnih programera.[51]

Iz gore spomenutih kvaziorganizacijskih obilježja, koja osobito dolaze do izražaja u načina na koji se postiže konsenzus, slijedi i da cijeli DLT/BC sustav ima zajedničku svrhu ili cilj, a to je zajedničko obavljanje usluge distribuiranoga knjiženja. Sudionici mreže su obvezni surađivati u postizanju zajedničkoga cilja kao biti odani jedni prema drugima, ali i odgovorni i jedni prema drugima, ali i prema trećima. Tu se postavlja pitanje može li se odnos sudionika DLT/BC mreže pravno kvalificirati kao

47 Zetzsche *et al.*, *The Distributed Liability*, 1386.

48 Zetzsche *et al.*, *The Distributed Liability*, 1387.

49 Zetzsche *et al.*, *The Distributed Liability*, 1389-1390.

50 V. Shawn J. Bayern, „Dynamic Common Law and Technological Change: The Classification of Bitcoin“, *Washington & Lee Law Review.* 71, br. 2 (2014): 31-33.

51 U prilog te odgovornosti izjašnjava se De Filippi za mrežu Ethereum, v. Primavera De Filippi, „Ethereum“, u: *Abécédaire des architectures distribuées*, ed. Cécile Méadel i Francesca Musiani (Paris: Presses des Mines, 2015.), 95-100. Aaron Wright, Primavera De Filippi, *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*, https://ssrn.com/abstract=2580664, 55 i dalje zalažu se za takvu odgovornost razvojnih programera, ali ne i običnih korisnika.

ortaštvo.[52] Kriteriji ortaštva variraju od poretka do poretka. Prema nekima je dostatan zajednički cilj te labava, faktična, organizacijska struktura.[53] Izraženo je stajalište da je rizik da se prema *common lawu* suradnja na BC mreži proglasi ortaštvom vrlo neznatan, dokle god se mogućnosti zarade nalaze u rukama trećih osoba, odnosno organizatora/sponzora same mreže, a čvorovi snose svoje vlastite troškove i bivaju nagrađeni kriptovalutom na predeterminiranoj osnovi.[54] Cilj ostvarenja dobiti koji je svojstven trgovačkim društvima ne mora biti cilj ortaštva, kao niti obavljanje gospodarske djelatnosti.

Kada je u pitanju DAO, s obzirom na to da se pri osnivanju DAO-a dolazi do emisije tokena, DAO nalikuje i na inicijalnu ponudu udjela u društvu s ograničenom odgovornošću, iako nema prepreka da ga se pravno kvalificira kao ortaštvo.[55] No, najvažnija posljedica pravne kvalifikacije kao ortaštva je ta da ortaštvo ne odgovara prema trećima kao jedan entitet, već svi ortaci odgovaraju pojedinačno (neograničeno i solidarno), uz pravo regresa prema ostalima. Opravdano se postavlja pitanje jesu li mali ulagatelji (koju primjerice ulažu u kriptovalute) svjesni da ušavši u DLT/BC mrežu preuzimaju tu vrstu odgovornosti. Za njih bi svakako bilo primjerenije da je odgovornost ograničena visinom uloga. No, unaprijed je nemoguće jednoznačno identificirati pravnu kvalifikaciju neke BC mreže, jer to ovisi i o pojedinačnim obilježjima te konkretne mreže, odnosno aplikacije na mreži. Kada BC mreže oponašaju trgovačka društva, puno bi prikladnije bilo da se u mreži sudionika izdvoje dvije kategorije ortaka, te da jedni odgovaraju neograničeno i solidarno, a drugi ograničeno do visine uloženog. To je model koji se u nas utjelovljuje u komanditnom društvu, no ono treba udovoljiti i formalnim zahtjevima osnivanja, a to bi u nas bio upis toga društva u registar. No, to je oblik ulaganja koji je karakterističan za fondovsku industriju.[56] Iz primjera je vidljivo da je DAO oblikovan upravo da se premoste neki nedostatci fondovskog ulaganja, koji se između ostalog sastoje u tome da se u modelu DAO-a održava kontrola nad time u što se ulaže. Pritom se pri fondovskom ulaganju ta briga prepušta menadžeru fonda, pri čemu se odnos između ulagatelja i menadžera

52 Kada je u pitanju DAO, on je nepobitno usporediv s ortaštvom uređen Zakonom o obveznim odnosima, Narodne novine, br. 35/05., 41/08., 125/11., 78/15., 29/18., 126/21. Svi ortaci solidarno odgovaraju vjerovniku za obveze ortaštva (čl. 648. ZOO). Detaljnu analizu pravne kvalifikacije DAO-a vidi u nas: Antun Bilić, „Legal status and corporate governance of decentralized autonomous organizations", u: *EU Financial Regulation and Markets: Beyond Fragmentation and Differentiation*, ur. Ivana Bajakić i Marta Božina Beroš (Zagreb: Pravni fakultet u Zagrebu, 2020.), 192-219.

53 Till Jaeger i Axel Metzger, *Open Source Software: rechtliche Rahmenbedingungen der freien Software*, 4. Aufl. (Muenchen: Beck C. H., 2016.), 193-200. Prema tim autorima razvojni programeri bili bi ortaci jer im je cilj razvijanje programa, a postoji labava organizacijska struktura. U zemljama *common law* sustava, bilo bi bitno i postoji li sporazum o podjeli dobiti. V. Zetzsche et al., *The Distributed Liability,* 1400.

54 Zetzsche *et al.*, *The Distributed Liability*, 1400.

55 V. detaljno Bilić, *Legal status,* 196 i dalje. Usp. Garcia Rolo, *Challenges in the Legal Qualification,* 64-68.

56 Odnedavno predviđen oblik fonda, s izmjenama Zakona o alternativnim investicijskim fondovima, Narodne novine, br. 110/21. Vidi čl. 99.a.

fonda kvalificira kao povjerenički odnos, temeljen na ugovoru.[57]

Ima pravnih sustava koji su omogućili kreiranje DLT/BC poslovnoga modela u obliku društva s ograničenom odgovornosti te mu dali pravnu osobnost. Primjer je nacionalno pravo države Vermont u SAD-u, koja je u 2018. donijela zakon kojim se uvodi novi oblik trgovačkog društva pod nazivom društvo s ograničenom odgovornošću utemeljeno na BC tehnologiji (engl, *blockchain-based limited liability company* - dalje: *BBLLC)*.[58] Prednosti dodjeljivanja pravne osobnosti su očite, od pravne osobnosti do ograničene odgovornosti ulagatelja. To je svakako na tragu postizanja veće pravne sigurnosti za ulagatelje u BC sustave, osobito za kategoriju, tzv. jednostavnih korisnika, koji u tom slučaju imaju štit ograničene odgovornosti za obveze takvog društva.

2.3.3. Posebno o uspostavi odgovornosti ključnih razvojnih programera

Odgovornost za hakerski napad koji je posljedica nedostataka u algoritamskom kodu [59] otvorila je u pravnoj doktrini SAD-a raspravu o tome može li se ta odgovornost pripisati ključnim razvojnim programerima, proglašavajući ih svojevrsnim fiducijarima DLT/BC sustava. Njihova fiducijarna odgovornost izvodila bi se iz njihove osobite stručnosti i utjecaja (engl. *influencers*) na javni BC. Walch je predložila da se programere koji predlažu ili zagovaraju promjene u algoritamskog koda javnog BC treba smatrati fiducijarima jer imaju premoć nad ostalim korisnicima. Oni *de facto* kontroliraju kod, odnosno njegove promjene, a to se izvodi iz utjecaja kojeg imaju na proces donošenja odluka.[60] Izvan SAD-a ta doktrina također nailazi na svoje uporište.[61] Prema Frankelu, uglednom akademskom stručnjaku za fiducijarno pravo, fiducijarne obveze tradicionalno nastaju u odnosima koji pokazuju dvije središnje karakteristike: fiducijar je povjerenik druge strane i pruža joj specijalizirane usluge koje su društveno važne i obično skupe. Da bi fiducijar to bio, druga mu strana mora prenijeti ili imovinu

57 V. čl. 91. st. 1. Zakona o otvorenim investicijskim fondovima s javnom ponudom, Narodne novine, br. 44/16., 126/19., 110/21.

58 11 V.S.A. § 4173 - potpoglavlje 012: *Blockchain-based Limited Liability Companies.*

59 Raspravu od tome koje pravo treba primijeniti na krađu kriptovaluta, obuhvaćaju između ostalog i pitanje smatraju li se prava imatelja digitalnog novčanika pravima *in rem* ili *in personam*. Vidi, Florence Guillaume, „Aspects of private international law related to blockchain transactions“, u: *Blockchains, smart contracts, decentralised autonomous organisations and the law,* eds. Daniel Kraus, Thierry Obrist i Olivier Hari (Northampton, MA: Edward Elgar Pub., 2019.), 62 i dalje.

60 Walch, *In Code(rs) we trust*, 65. Autorica to izvodi iz četiri ključne pretpostavke koje su potrebne za nametanje fiducijarnih obveza. Tvrdi da ključni razvojni programeri pružaju socijalno poželjnu uslugu koja zahtijeva posebnu ekspertizu (i), povjerena im je imovina ili su im dane ovlasti (ii), u mogućnosti su da taj svoj poseban položaj zloupotrijebe, odnosno da iznevjere povjerenje koje im je dano (iii), a osobe koje su im dale povjerenje ne mogu se zaštititi od njihovih radnji ili propusta (iv).

61 Xinyu Shi, *Do Core Developers Owe Fiduciary Duty to Users of Blockchain Platforms?,* https://ssrn.com/abstract=3526685. Autorica smatra da su prednosti uspostave fiducijarne obveze ključnih razvojnih programera, veće od nedostataka, jer bi potonja obveza pomogla u izgradnji povjerenja javnosti u BC. Iz kuta lihtenštajnskog prava, v. Elisabeth M. S. Frommelt, „Liability Challenges in the Blockchain Ecosystem“, *UC Davis Business Law Journal* 21, br. 1 (2020-2021): 165-222.

ili ovlasti povjerenika.[62] No, to ujedno ne znači da će svako povjeravanje imovine ili ovlasti uroditi fiducijarnim obvezama. Ako već postoje pravni zaštitni mehanizmi koji će na prikladan način ukloniti rizik zlouporabe diskrecijskih ovlasti fiducijara, tada nema potrebe za fiducijarnom obvezom.[63]

Protivnici ove odgovornosti tvrde da prije negoli što se ključne razvojne programere proglasi fiducijarima, treba imati hrabrosti i spremnosti da se pomno ispitaju razlike u položaju ključnih razvojnih programera u odnosu na direktore korporacije s čijim ih se fiducijarnim dužnostima najčešće uspoređuje.[64] No, ovlasti direktora nastaju kao posljedica „razdvajanja vlasništva od kontrole" (engl. *agency problem*), odnosno slijedom činjenice da dioničari / članovi društva imenuju direktore kao osobe koje vode poslove društva i zastupaju društvo.[65] Sudovi su skloni nametnuti fiducijarne dužnosti direktorima tražeći od njih da zaštite interese društva i da djeluju u najboljem interesu dioničara,[66] a mogu čak obvezati društvo i protiv volje oponirajućih dioničara.[67] Također se tvrdi da su dužnosti članova uprave prema dioničarima izgubile na svojoj fiducijarnoj težini, te su postale skup prilično uskih i specifičnih dužnosti definiranih između ostalog i složenom mrežom osiguranja od odgovornosti.[68]

No, što protivnici ističu kao razlike? Ključni razvojni programeri nisu zastupnici (engl. *agents*) ikojega drugog sudionika mreže, bilo pojedinačno ili kolektivno. Programeri protokola ne mogu obvezati ikojeg sudionika mreže na promjenu softverske aplikacije. Sudionik mreže, s druge strane nema moć usmjeravanja ili kontrole radnji programera protokola. Tvrde da je doprinos programera inherentno drukčiji u proizvodnji algoritamskog koda jer je dobrovoljan, suradnički i ponavljajući. Pritom osobito ističu da je javnim BC mrežama svojstven otvoreni sustav proizvodnje koda (engl. *open source*).[69] Riječ je o proizvodnji koda putem dobrovoljnoga sudjelovanja

62 Tamar Frankel, „Fiduciary Law", *California Law Review* 71, br. 3 (1983): 808.

63 Frankel, *Fiduciary Law*, 808, 811.

64 Haque et al., *Blockchain Development*, 174.

65 Ta je ovlast propisana u čl. 141. Općeg zakona o korporacijama savezne države Delaware (u daljnjem tekstu: *Delaware General Corporation Law*).

66 Tako je u sudskoj praksi potvrđeno da direktori imaju fiducijarne obveze i prema dioničarima redovitih i povlaštenih dionica (predmet Arnold v. Soc'y for Sav. Bancorp, Inc., 678 A.2d 533, 539, Del. 1996). No, ako se interesi tih dioničara razlikuju, tada se fiducijarna obveza duguje samo dioničarima redovitih dionica (predmet Trados Inc. S'holder Litig., 2009 WL 2225958, Del. Ch. July 24, 2009).

67 Gabriel Shapiro, *Supplemental Rebuttal to Angela Walch's Views on Software Devs as Fiduciaries*, https://lex-node.medium.com/supplemental-rebuttal-to-angela-walchs-views-on-software-devs-as-fiduciaries-f886f2b47ffd.

68 U predmetu Smith v. Van Gorkom 488 A.2d 858, Del. 1985., Vrhovni je sud države Delaware smatrao članove upravnog odbora ciljnog društva odgovornima za pregovore pri (dobrovoljnom) preuzimanju, odnosno da vođenjem pregovora na krajnje nemaran način krše fiducijarnu obvezu (engl. *duty of care*). Posljedica je ovoga predmeta slabljenje fiducijarnih obveza jer je članak 102(b)(7) Delaware General Corporation Law, otvorio mogućnost oslobođenja direktora od fiducijarnih obveza.

69 U tom sustavu programeri se nalaze na različitim lokacijama. Jean Tirole i Josh Lerner, „The Simple Economics of Open Source", *HBS Finance Working Paper* br. 2000–059., https://ssrn.com/abstract=224008, 1.

decentraliziranih sudionika.[70] Svakome je dopušteno predložiti promjenu koda zajednici, a također je dopušteno izmijeniti postojeći kod i pokušati izgraditi vlastitu zajednicu kako bi podržala revidiranu verziju koda. To što programeri protokola katkad „govore za zajednicu" u javnim nastupima i na sastancima s javnim dužnosnicima, oponenti smatraju nedostatnim za uspostavu fiducijarne obveze.

Protivnici tvrde da se odnos između ključnoga programera BC protokola i običnog imatelja tokena uspostavlja na temelju dviju odvojenih radnji: odluke razvojnoga programera protokola da doprinese razvoju koda i odluke druge osobe da sudjeluje u javnom BC-u putem stjecanja tokena ili putem upravljanja čvorom. Zaključuju da niti jedna od ovih radnji sama za sebe ili u kombinaciji s drugom ne implicira fiducijarni odnos. Zalažu se za analognu primjenu zaštitnih mehanizama iz drugih pravnih područja (iz prava vrijednosnih papira ili platnih transakcija) na novu tehnološku podlogu umjesto konstruiranja novih fiducijarnih obveza.[71]

Doktrinarna shvaćanja iz pera europskih autora, također ne nude jednoznačne odgovore o odgovornosti ključnih razvojnih programera. Potvrđuju da oni jesu svojevrsni usmjerivači (engl. *policy makers*) javnog BC-a, te da prate njegov razvoj.[72] Predlažu rješenja koja se odnose na funkcionalnost BC sustava i primjenjiva načela BC-a, o kojima onda rudari glasuju.[73] Frommelt tvrdi da razvojni programeri mogu doista uvelike utjecati na BC sustav. Također tvrdi da bi se njima mogla pripisati odgovornost za ispravno funkcioniranje BC sustava, ali uz pretpostavku da oni jesu jedno središnje mjesto u sustavu, što se naravno protivi ideji istorazinske suradnje na kojoj počiva BC.[74]

Ipak, kako razvojni programeri mogu biti izravno nagrađeni tokenima za svoj doprinos zajedničkom cilju,[75] postoji prostor za njihovu pristranost u promišljanju strategija oporavka od napada na sustav. Razvojni programeri mogu zagovarati rješenja kojima će svoje interese pretpostaviti interesima drugih korisnika. Stoga je u akademskoj zajednici otvorena rasprava i o etičkoj odgovornosti ključnih razvojnih programera.[76] Zbog široke primjene, kao i zbog temeljnih osobina novih tehnoloških rješenja, nužno je razmotriti kako će se s tim izazovima nositi trgovačka društva koja će biti, ili već jesu, njihovi korisnici.

70 Rodrigo Seira Silva-Herzog, *Blockchain Protocol Developers are not Fiduciaries: An Analysis of the Cryptoeconomics of Open Source Networks and the Role of Protocol Developers in Public Blockchain Network Governance* (2018), https://blog.goodaudience.com/blockchain-protocol-developers-are-not-fiduciaries-49bf436a20ca#_ftn24.

71 Haque et al., *Blockchain Development*, 182.

72 Michèle Finck, *Blockchain Regulation and Governance in Europe* (Cambridge: Cambridge University Press, 2018., 52.

73 Finck, *Blockchain Regulation*, 52.

74 Frommelt, *Liability Challenges*, 187.

75 Seira Silva-Herzog, *Blockchain Protocol Developers*, poglavlje II.d.

76 Neitz, *The Influencers*, 18.

3. KOME U TRGOVAČKOM DRUŠTVU POVJERITI BRIGU O ODABIRU BC TEHNOLOGIJE

Trgovačka društva, osobito velika i gospodarski jaka (dionička) društva, zbog imperativa inovativnosti koji je ključan sastojak kompetitivnosti sve će češće posezati za primjenom BC tehnologija. Stoga je primjenu BC tehnologije nužno razmotriti i iz perspektive trgovačkoga društva, kao naručitelja novog BC rješenja. Postavlja se pitanje tko bi u trgovačkom društvu trebao biti nadležan za odobravanje i praćenje primjene novih tehnoloških rješenja zbog novih sukoba interesa koji se mogu pojaviti.

Pritom se misli na to da zaposlenici društva, koji daju podatke ili utječu na izradu novoga tehnološkog rješenja mogu biti u iskušenju da ga prilagode sebi, posebno ako će ono utjecati na njihovo nagrađivanje.[77] Primjerice, ako se razvija BC program koji bi trebao u sustav poslati znakove upozorenja o opasnosti nastupa nekog rizika, a upozorenja budu poslana prekasno, to može s jedne strane štetiti društvu, a s druge pogodovati zaposleniku, koji će za dobro upravljanje rizicima biti i nagrađen. Zbog nedostatnog znanja o novim tehnologijama nerijetko u društvu nije moguće niti pronaći osobu čije će kompetencije ići u korak s isporučiteljima BC tehnoloških rješenja. Zbog toga je nužno u proces odabira i/ili kontrole BC rješenja uključiti nepristrane, etički osviještene tehnološke stručnjake. Osim zaposlenika, sukobi interesa su i na strani isporučitelja BC rješenja. Svjesni tko odlučuje u društvu o prihvaćanju ponude, njihovi kreatori mogu *sua sponte* prilagoditi rješenja interesima osoba koje o prihvaćanju ponude donose odluke.[78] Tu je i rizik koluzivnoga djelovanja zaposlenika i dobavljača digitalnog alata, a na štetu društva.[79]

Korporativna praksa ne daje još dostatno čvrste odgovore čija bi to bila briga u društvu. Ako u društvu (misli se ponajprije na veća i jača dionička društva, osobito financijske institucije) djeluju uredi koji se bave očuvanjem integriteta informacijskog sustava (engl. *chief information officer*) i tehnološki odbori uprave ili nadzornih odbora, to bi mogao biti njihov zadatak. Njihova je temeljna zadaća zaštita od hakerskih napada ili preveniranje nastupa operativnih rizika povezanih s tehnološkim rješenjima.[80] Prethodno opisani slučajevi napada zasigurno bi bili predmet njihova interesa. Zbog toga Enriques i Zetzsche predlažu da tehnološki odbori budu *ex ante* osnaženi mogućnošću da nadziru i proces pregovaranja s programerima, upravljaju ugovornim odnosom, pregledavaju postavke dizajna ključnih algoritama i sl. No također, svjesni da bi taj prijedlog mogao smanjiti poslovnu učinkovitost, rješenje ipak vide u jačanju nadzornih ovlasti tehnološkog odbora, ali ne nužno *ex ante*.[81] Prema tome jedno je od mogućih rješenja osnažiti tehnološki odbor.

77 Enriques *et al.*, *Corporate Technologies*, 38.

78 Enriques *et al.*, *Corporate Technologies*, 38.

79 Enriques *et al.*, *Corporate Technologies*, 51.

80 Max Bankewitz, Carl Åberg i Cristine Teuchert, „Digitalization and Boards of Directors: A New Era of Corporate Governance?“, *Business and Management Research* 20, br. 5 (2016): 65. Glavna je zadaća tog odbora, primjerice potvrditi da struktura informacijskog sustava podržava strategiju društva, provjeriti jesu li alati za sigurnost podataka učinkoviti, kao i jesu li učinkovite akcije koje se poduzimaju u povodu kršenja sigurnosti podataka i sl.

81 Enriques *et al.*, *Corporate Technologies*, 54.

Drugo je rješenje, staviti ovo pitanje u nadležnost tijela koje se općenito bavi sprječavanjem i upravljanjem sukoba interesa u trgovačkom društvu. To može biti stavljeno u nadležnost uredu za usklađenost, posebice ako se njegova uloga promatra ne samo kao postizanje usklađenosti trgovačkog društva s primjenjivim propisima, već i sa zahtjevima etičnog ponašanja koje podrazumijeva sprječavanje, odnosno upravljanje sukobom interesa.[82] Također je moguće da to bude i služba unutrašnje kontrole[83] ili ured za praćenje usklađenosti koji prijavljene sukobe interesa, i njihove povrede proslijeđuje unutrašnjoj reviziji.[84] Imajući u vidu da se sve više otvara i etički diskurs u brojnim aspektima primjene BC tehnologije, čini se da bi se problemi oko odabira i praćenja provedbe naprednih tehnoloških rješenja u trgovačkom društvu mogli riješiti suradnjom tehnološkog odbora, ako takav postoji, i ureda za usklađenost.

Međutim, nužno je napomenuti da kolikogod bila napredna inozemna korporativna praksa, uredi za usklađenost ne postoje u svim trgovačkim društvima, osim, u društvima čiji je većinski dioničar/udjelničar RH,[85] kao i u financijskom sektoru.[86] Trgovačko je društvo svakako slobodno samo odrediti mjesto tim pitanjima u mozaiku korporativnog upravljanja, jer nije riječ o unaprijed zadanoj veličini, osim ako je u pitanju sukob interesa u kojem se nalazi član uprave.[87]

4. ZAKLJUČAK

BC ima široku primjenu u poslovanju trgovačkog društva, kao i u korporativnom upravljanju. Kako je BC tehnologija podnormirana, u slučaju zlouporabe pojavljuju se mnoga otvorena pitanja. U ovom su radu analizirana dva slučaja u kojima je javni BC pretrpio napad izvana, te su pri oporavku sustava primijenjene različite metode u sličnim situacijama. To je dalo povoda općoj raspravi o tome na koji način upravljački funkcionira BC zajednica te koju ulogu u procesu imaju ključni razvojni programeri i mogu li oni biti odgovorni za nastup toga rizika.

U pravnoj doktrini vode se rasprave o tome trebaju li se ključni razvojni programeri upravo zbog mjere njihova utjecaja smatrati novim fiducijarima, odnosno

82 Morana Derenčinović Ruk, *Razvoj i pravno uređenje sukoba interesa i instituta usklađenosti na hrvatskom tržištu kapitala: (doktorska disertacija)* (Zagreb: Pravni fakultet u Zagrebu, 2016.), 21. V. još Edita Čulinović-Herc i Sara Madžarov Matijević, „Companies in the blockchain era - importance of corporate culture“, u: eds. Gerald G. Sander, Ana Pošćić i Adrijana Martinović, *Exploring the Social Dimension of Europe, Essays in Honour of Nada Bodiroga-Vukobrat* (Hamburg: Verlag Dr. Kovač, 2021.), 453-456.

83 Vidi čl. 15. Politika upravljanja sukobom interesa, Imperial Riviera d.d., Poreč, 2020., 8 kao i čl. 15. Politika upravljanja sukobom interesa, Jadran d.d., Crikvenica, 2021., 8.

84 Vidi čl. 8. i 11. st. 2. Politike upravljanja sukobom interesa, PBZ, d.d. Zagreb, 2019., 12-13.

85 Odluka o obvezi uvođenja funkcije praćenja usklađenosti poslovanja u pravnim osobama u većinskom državnom vlasništvu, Narodne novine, br. 99/19.

86 Npr. za društva za upravljanje investicijskim fondovima. Obveze proizlaze iz Zakona o otvorenim investicijskim fondovima s javnom ponudom, Narodne novine, br. 44/16., 126/19., 110/21. i Pravilnika o organizacijskim zahtjevima za društva za upravljanje UCITS fondovima, Narodne novine, br. 41/17.

87 Čl. 248.a Zakona o trgovačkim društvima, Narodne novine, br. 111/93., 34/99., 121/99., 52/00., 118/03., 107/07., 146/08., 137/09., 125/11., 152/11., 111/12., 68/13., 110/15., 40/19., 34/22.

treba li ih kvalificirati kao povjerenike kojima se povjerava imovina ili dodjeljuju povjereničke ovlasti. Zagovaratelji ovog stava tvrde da je uloga ključnih razvojnih programera u bitnome slična ulozi korporativnih direktora koja nastaje kao posljedica „razdvajanja vlasništva od kontrole" (engl. *agency problem*), odnosno činjenice da dioničari/članovi društva imenuju direktore kao osobe koje vode poslove društva i zastupaju društvo. Oponenti smatraju da će širenje toga koncepta odgovornosti kroz sudsku praksu, zaustaviti temeljnu inovaciju BC tehnologije, koja proizlazi iz činjenice da se programi kodiraju u otvorenom pristupu te da u njemu ključni razvojni programeri sudjeluju na participirajući, istorazinski i opetujući način. Iz toga oponenti izvode daljnju tezu da ključni razvojni programeri ne bi mogli biti fiducijari jer im nedostaje temeljna pretpostavka, a to je da je njima povjerena imovina ili su im dane povjereničke ovlasti. Ipak, uvid u dva slučaja napada na javni BC pokazao je da su ključni razvojni programeri itekako utjecali na primjenu metode oporavka. Oponenti, pak upozoravaju da će primjena fiducije dovesti do uništenja *open source* modela kodiranja.[88]

Kada se rizici primjene DLT/BC tehnologije sagledaju iz kuta trgovačkog društva, kao naručitelja novih tehnoloških rješenja uočeno je nekoliko točaka u mozaiku korporativnog upravljanja (osobito dioničkih društava) čija bi to mogla biti nadležnost. Kao prvo to bi mogao biti tehnološki odbor (ako takav postoji). Njega bi trebalo osnažiti ovlastima koje će mu omogućiti da utječe na pregovore, odabir ponuđača, odabir dizajna novoga tehnološkog rješenja ili mu barem pridjenuti određene nadzorne ovlasti. Taj bi se zadatak mogao povjeriti i uredu za usklađenost, iako taj ured / funkcija ne postoji u organigramu svih većih društava, već primarno u društvima čiji je većinski dioničar RH, kao i u financijskim institucijama. Ured za usklađenost prikladan je zbog toga jer njegova zadaća nije samo voditi brigu o postizanju usklađenosti trgovačkog društva s primjenjivim propisima, već i sa zahtjevima etičnog ponašanja, odnosno sprječavanja sukoba interesa kakvih tu ima. Također se prijava nepravilnosti može povjeriti i službi unutrašnje kontrole. Na taj zaključak upućuju i analizirane politike upravljanja sukobom interesa nekih dioničkih društava.

LITERATURA

Knjige i članci:

1. Antonopoulos, Andreas i Gavin Wood. *Mastering Ethereum: building smart contracts and DApps*. Cambridge: O'Reilly, 2018.
2. Bamberger, Kenneth. „Technologies of Compliance: Risk and Regulation in a Digital Age". *Texas Law Review* 88, br. 4 (2010): 669-739.
3. Bankewitz, Max, Carl Åberg i Cristine Teuchert. „Digitalization and Boards of Directors: A New Era of Corporate Governance?". *Business and Management Research* 20, br. 5 (2016): 58-69.
4. Bayern, Shawn J. „Dynamic Common Law and Technological Change: The Classification of Bitcoin". *Washington. & Lee Law Review. Online* 71, br. 2 (2014): 23-34.
5. Bilić, Antun. „Legal status and corporate governance of decentralized autonomous

88 Haque *et al.*, *Blockchain Development*, 186.

organizations“. U: EU Financial Regulation and Markets: Beyond Fragmentation and Differentiation, ed. Ivana Bajakić, Marta Božina Beroš, 192-219. Zagreb: Pravni fakultet u Zagrebu, 2020.

6. Buterin, Vitalik. *Letter of 19th of July 2021*, https://twitter.com/VitalikButerin/status/887783867129745412
7. Čulinović-Herc, Edita i Sara Madžarov Matijević. „Companies in the blockchain era - importance of corporate culture“. U: ed. G.G. Sander, Ana Pošćić and A. Martinović. *Exploring the Social Dimension of Europe, Essays in Honour of Nada Bodiroga-Vukobrat*, 453-456. Munchen: Verlag Dr. Kovač, 2021.
8. De Filippi, Primavera i Aaron Wright. *Blockchain and the Law - The Rule of Code, Cambridge*. London: Harvard University Press, 2018.
9. Del Castillo, Michel. *Ethereum Executes Blockchain Hard Fork to Return DAO Funds*, https://www.coindesk.com/tech/2016/07/20/ethereum-executes-blockchain-hard-fork-to-return-dao-funds
10. Derenčinović Ruk, Morana. *Razvoj i pravno uređenje sukoba interesa i instituta usklađenosti na hrvatskom tržištu kapitala: doktorska disertacija*. Zagreb: Pravni fakultet u Zagrebu, 2016.
11. Enriques, Luca i Dirk A. Zetzsche. „Corporate Technologies and the Tech Nirvana Fallacy“. *European Corporate Governance Institute - Law Working Paper* br. 457 (2019): 1-65., http://dx.doi.org/10.2.139/ssrn.3392321
12. Fenwick, Mark i Erik P. M. Vermeulen. „The New Firm: Staying Relevant, Unique and Competitive“. *European Business Organization Law Review* 16, br. 4 (2015): 595-623.
13. Finck, Michèle. *Blockchain Regulation and Governance in Europe*. Cambridge: Cambridge University Press, 2018.
14. Frankel, Tamar. „Fiduciary Law“. *California. Law. Review.* 71, (1983): 795-836.https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=2137&context=californialawreview
15. Frommelt, Elisabeth M. S. „Liability Challenges in the Blockchain Ecosystem“. *UC Davis Business Law Journal* 21, br. 1. (2020-2021): 165-221.
16. Gabriel Shapiro. *Supplemental Rebuttal to Angela Walch's Views on Software Devs as Fiduciaries*, https://lex-node.medium.com/supplemental-rebuttal-to-angela-walchs-views-on-software-devs-as-fiduciaries-f886f2b47ffd
17. Garcia Rolo, Antonio. „Challenges in the Legal Qualification of Decentralised Autonomous Organisations (DAOs): The Rise of the Crypto-Partnership?“. *Revista de Direito e Tecnologia* 1, br. 1 (2019): 33-87.
18. Gazi Güçlütürk, Osman. *The DAO Hack Explained: Unfortunate Take-off of Smart Contracts*. https://ogucluturk.medium.com/the-dao-hack-explained-unfortunate-take-off-of-smart-contracts-2bd8c8db3562
19. Guillaume, Florence. „Aspects of private international law related to blockchain transactions“, u: *Blockchains, smart contracts, decentralised autonomous organisations and the law*, eds. Daniel Kraus, Thierry Obrist i Olivier Hari, 49-82. Northampton, MA: Edward Elgar Pub., 2019.
20. Haque, Raina S., Rodrigo Seira Silva-Herzog, Brent A. Plummeri i Nelson M. Rosario. „Blockchain Development and Fiduciary Duty“. *Stanford. Journal of Blockchain Law & Policy*. 2, (2019): 139-187.
21. Hirsch, David. „Blockchain and Information Security“. U: Handbook of Blockchain law, eds. Matthias Artzt i Thomas Richter, 77-122. The Hague: Wolters Kluwer, 2020.
22. Jaeger, Till i Axel Metzger. *Open Source Software: rechtliche Rahmenbedingungen der freien Software*. 4. Aufl. Muenchen: Beck C. H., 2016.
23. Karapetsas. *Lefteris How to split the DAO*, https://github.com/slockit/DAO/wiki/How-to-split-the-DAO

24. Kaulartz, Markus i Jörn Heckmann. „Smart Contracts – Anwendungen der Blockchain-Technologie". *Computer und Recht* 32, br. 9 (2016): 618-624.
25. Leising, Matthew. *The Ether Thief, Bloomberg, June 13, 2017*, https://www.bloomberg.com/features/2017-the-ether-thief/
26. Madeira, Antonio. *The Dao, the Hack, the Soft Fork and the Hard Fork*, https://www.cryptocompare.com/coins/guides/the-dao-the-hack-the-soft-fork-and-the-hard-fork/
27. Neitz, Michele B. „The Influencers: Facebook's Libra, Public Blockchains, And the Ethical Considerations of Centralization". *North Carolina Journal of Law & Technology.* 21, br. 2 (2019): 1-28.
28. *OECD Studies on SMEs and Entrepreneurship Understanding Firm Growth Helping SMEs Scale Up*. Paris: OECD, 2021.
29. Parity Technologies. *The Multi-sig Hack: A Postmortem*, https://www.parity.io/blog/the-multi-sig-hack-a-postmortem
30. Seira, Rodrigo. *Blockchain Protocol Developers are not Fiduciaries: An Analysis of the Cryptoeconomics of Open Source Networks and the Role of Protocol Developers in Public Blockchain Network Governance*, Nhttps://blog.goodaudience.com/blockchain-protocol-developers-are-not-fiduciaries-49bf436a20ca#_ftn24
31. Shein, Esther. *How Blockchain Changes the Nature of Trust, Linux Foundation*, https://linuxfoundation.org/blog/how-blockchain-changes-the-nature-of-trust/
32. Shi, Xinyu. *Do Core Developers Owe Fiduciary Duty to Users of Blockchain Platforms?,* https://ssrn.com/abstract=3526685
33. Siegel, David. *Understanding The DAO Attack*, https://www.coindesk.com/learn/2016/06/25/understanding-the-dao-attack/
34. Szabo, Nick. *Smart contracts, 1994.* https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html
35. Tirole, Jean i Josh, Lerner. „The Simple Economics of Open Source (October 2000)". *HBS Finance Working Paper* br. 00–059., https://ssrn.com/abstract=224008
36. Tomaino, N., *The Governance of Blockchains*, https://thecontrol.co/the-governance-of-blockchains-5ba17a4f5da6
37. Trillmich, Philip, Matthias Goetz i Chris Ewing. „Blockchain and Smart Contracts". U: Handbook of Blockchain law, eds. Matthias Artzt i Thomas Richter, 163-192. The Hague: Wolters Kluwer, 2020.
38. Tse, Nathan. „Decentralised Autonomous Organisations and the Corporate Form". *Victoria University of Wellington Law Review* 51, br. 3 (2020): 319.
39. Van der Laan, Jake. „Understanding Blockchain". U: Handbook of Blockchain law, eds. Matthias Artzt i Thomas Richter, 1-75. The Hague: Wolters Kluwer, 2020.
40. Walch, Angela. „In Code(rs) we trust: Software developers as fiduciaries in public blockchains". U: *Regulating Blockchain: Techno-Social and Legal Challenges*, Philipp Hacker, Ioannis Lianos, Georgios Dimitropoulos i Stefan Eich, 59-75. Oxford: Oxford Scholarship online, 2019.
41. Walch, Angela. „The Bitcoin Blockchain as Financial Market Infrastructure: A Consideration of Operational Risk". *N.Y.U. Journal of Legislation and Public Policy* (2015): 859-865.
42. Werbach, Kevin. „Trust, but Verify: Why Blockchain Needs the Law". *Berkeley Technology Law Journal.* 33, br. 2 (2018): 487-550.
43. Wright, Aaron i Primavera De Filippi. *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*, https://ssrn.com/abstract=2580664, 1-58.
44. Zetzsche, Dirk A., Ross Buckley i Arner Douglas. „The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain". *University of Illinois Law Review* br. 4 (2018): 1382-1402.

Propisi i autonomni izvori prava RH:

1. Odluka o obvezi uvođenja funkcije praćenja usklađenosti poslovanja u pravnim osobama u većinskom državnom vlasništvu, Narodne novine, br. 99/19.
2. Politika upravljanja sukobom interesa, Imperial Riviera d.d., Poreč, 2020., str. 8.
3. Politika upravljanja sukobom interesa, Jadran d.d., Crikvenica, 2021., str. 8.
4. Politika upravljanja sukobom interesa, PBZ, d.d. Zagreb, 2019., str. 12-13.
5. Pravilnik o organizacijskim zahtjevima za društva za upravljanje UCITS fondovima, Narodne novine, br. 41/17.
6. Zakon o alternativnim investicijskim fondovima, Narodne novine, br. 21/18., 126/19., 110/21.
7. Zakon o obveznim odnosima, Narodne novine, br. 35/05., 41/08., 125/11., 78/15., 29/18., 126/21.
8. Zakon o otvorenim investicijskim fondovima s javnom ponudom, Narodne novine, br. 44/16., 126/19., 110/21.
9. Zakon o trgovačkim društvima, Narodne novine, br. 111/93., 34/99., 121/99., 52/00., 118/03., 107/07., 146/08., 137/09., 125/11., 152/11., 111/12, 68/13., 110/15., 40/19., 34/22.

Inozemni propisi:

1. Blockchain-based Limited Liability Companies 11 V.S.A. § 4173
2. State of Delaware General Corporation Law, 83 Del. Laws, c. 280.

Sudska praksa:

1. Arnold v. Soc'y for Sav. Bancorp, Inc., 678 A.2d 533, 539 (Del. 1996)
2. Re Trados Inc. S'holder Litig., 2009 WL 2225958 (Del. Ch. July 24, 2009)
3. Smith v. Van Gorkom, 488 A.2d 858 (1985)

Edita Čulinović-Herc*

Summary

ABUSES OF BLOCKCHAIN TEHNOLOGY AND IMPACT ON COMPANIES

Blockchain technology (hereinafter: BC), which is classified as distributed ledger technology (hereinafter: DLT), has a wide application in operation of business as well as in corporate governance. It is under-regulated, tends to function extra-institutionally and it could be source of abuse/misuse. The paper analyzes two cases of the abuse of BC technology, the risks that have arisen, as well as recovery methods that were applied. While it is widely discussed to whom those risks should be attributed, a concept of proclaiming core developers of the BC as fiduciaries was investigated thereby holding them liable for proper functioning of BC solution. Assesment of the same risks DLT / BC technologies were then viewed from the angle of the company, as potential purchaser of BC technological solutions from third party provider. A paper finally proposes who should in the company take care of the application of new BC technological solutions and ensure that those risks are prevented and/or efficiently managed in the company.

Keywords: *blockchain technology; misuse of BC technology; companies; responsibility of key developers.*

* Edita Čulinović-Herc, Ph.D., Full Professor, University of Rijeka, Faculty of Law; edita@pravri.hr. ORCID ID: orcid.org/0000-0002-6177-8057.
This paper was funded by project of University of Rijeka *Legal Aspects of Commercial Restructuring societies and the transition to a new culture of corporate governance* (uniridrustv-18-43).