VLOGA VERIŽNIH ORAKLJEV PRI PAMETNIH POGODBAH

MATIJA DAMJAN
Univerza v Ljubljani, Pravna fakulteta, Ljubljana, Slovenija.
E-pošta: matija.damjan@pf.uni-lj.si

Povzetek Tehnologija veriženja podatkovnih blokov omogoča sklepanje pametnih pogodb, ki se izvršijo samodejno, ko so za to izpolnjeni s pogodbo določeni pogoji. Vendar je blokovna veriga izolirano okolje in lahko potrdi le veljavnost podatkov, ki so vsebovani v sami verigi. Pri pametnih pogodbah, ki za svojo izpolnitev potrebujejo dostop do podatkov izven blokovne verige ali ki se celo izpolnijo zunaj verige, je tehnično nujno sodelovanje verižnega oraklja, ki deluje kot posrednik med blokovno verigo in resničnim svetom. Glede na tehnologijo ločimo med programskimi, strojnimi in človeškimi oraklji, glede na smer posredovanja podatkov pa med vhodnimi in izhodnimi oraklji. Tehnologija blockchain zagotavlja samo nespremenljivost podatkov, ne pa tudi njihove resničnosti, zato je nujno, da stranki oraklju zaupata ter da je pogodbeno zagotovljen njegov neodvisen in nepristranski položaj. Prispevek razpravlja o pravnem razmerju med strankami pametne pogodbe na eni strani in orakljem na drugi strani ter o ureditvi vloge oraklja v sami pametni pogodbi. V primerih, ko orakljeva storitev odpove, je pomembno, da je pametna pogodba tudi pravno zavezujoča.

Ključne besede: verižni orakelj, blockchain, pametna pogodba, samoizvršljiva pogodba, samodejna izvršitev pogodbe, podatki iz resničnega sveta.

Univerzitetna založba Univerze v Mariboru

DOI https://doi.org/10.18690/978-961-286-366-1.6
ISBN 978-961-286-366-1

THE ROLE OF BLOCKCHAIN ORACLES IN SMART CONTRACTS

MATIJA DAMJAN
Univetrsity of Ljubljana, Faculty of Law, Ljubljana, Slovenia.
E-mail: matija.damjan@pf.uni-lj.si

Abstract Blockchain technology allows parties to conclude smart contracts that are executed automatically when conditions specified in the contract are met. However, a blockchain is an isolated environment and can only validate the date contained in the chain itself. For smart contracts that require access to external data or need to be executed off-chain, it is technically necessary for an oracle to act as an intermediary between the blockchain and the real world. Depending on the technology, we can distinguish between software, hardware and human oracles, whereas the distinction between inbound and outbound oracles is based on the direction of data flow. Blockchain technology only ensures that data entered has not been subsequently modified, but it cannot guarantee that it is true. Therefore, the parties to a smart contract must trust the oracle and ensure that its independent and impartial position is contractually guaranteed. The article discusses the legal relationship between the parties to a smart contract on the one hand and the oracle on the other, and the regulation of the role of the oracle in the smart contract itself. When the oracle's service fails it is essential that the smart contract is also legally binding.

Keywords: blockchain oracle, smart contract, self-executing contract, automated performance, real-world data.

https://doi.org/10.18690/978-961-286-366-1.6 DOI
978-961-286-366-1 ISBN
University of Maribor Press

1 Uvod

Uporaba tehnologije veriženja podatkovnih blokov (blockchain) naj bi omogočila sklepanje pametnih pogodb, ki se izvršijo samodejno in tako zmanjšajo možnost neizpolnitve ter z njo povezanih sporov (Fries, 2018: 86). V verigo blokov je namreč mogoče vključiti programske algoritme, ki samodejno izvršijo določene transakcije (npr. izvedejo plačilo), ko so za to izpolnjeni s pogodbo dogovorjeni pogoji. Hkrati blokovna veriga zagotavlja, da se podatki o izvedenih transakcijah naknadno ne morejo spremeniti (De Filippi in Wright, 2018: 35 in 43). Tehnologija blockchain bi tako lahko omogočila strankam, ki se med seboj ne poznajo oz. si ne zaupajo, da neposredno sklepajo posle brez zanašanja na tretje osebe (npr. banke ali notarje) za zavarovanje izpolnitve. Zmanjšanje možnosti neizpolnitve bi zmanjšalo tudi potrebo po uporabi mehanizmov za reševanje sporov.

Vendar se pri napovedovanju revolucionarnih sprememb, ki naj bi jih na pravno področje prinesla tehnologija blockchain, pogosto spregleda, da ta tehnologija lahko potrdi le veljavnost podatkov, ki so vsebovani v sami verigi, in da lahko samodejno prenese le digitalne žetone, ki na blokovni verigi lahko predstavljajo določena sredstva ali pravice. Če je predmet pametne pogodbe dobava blaga ali opravljanje storitev v resničnem svetu, blokovna veriga ne more sama preveriti pravilnosti izpolnitve (npr. količine in kakovosti dobavljenega blaga), ampak mora to storiti nekdo tretji in ustrezen podatek posredovati v verigo (De Filippi in Wright, 2018: 75). Tehnologija zagotavlja, da ta podatek naknadno ne bo spremenjen, ne pa tudi, da je podatek resničen. Zato morata pogodbeni stranki zaupati agentu, ki bo preveril pravilnost izpolnitve pametne pogodbe v resničnem svetu. Izraz verižni orakelj (blockchain oracle) se uporablja za označevanje tovrstnih agentov, pooblaščenih za posredovanje dejanskih podatkov med resničnim svetom in blokovno verigo, zlasti zunanjih podatkov, ki naj sprožijo izvršitev pametne pogodbe. Ker je na tej točki izvršitve pametne pogodbe možnost zlorabe največja, je jasna pogodbena ureditev položaja verižnega oraklja bistvenega pomena. V prispevku razpravljam o vlogi in vrstah verižnih orakljev glede na različne vrste izpolnitev pri pametnih pogodbah ter o možnih pogodbenih okvirih opredelitve njihovih nalog.

2 Tehnične in pravne značilnosti pametnih pogodb

Pametna pogodba, kot jo je že sredi devetdesetih let opredelil *Nick Szabo*, obsega niz obveznosti, zapisanih v digitalni obliki, ki vključuje tudi protokole za njihovo izvršitev. Pogodbene zaveze naj bi se torej vgradile v programsko in strojno opremo, tako da bi njihova kršitev postala skorajda nemogoča (Szabo, 1996). Tehnologija veriženja podatkovnih blokov, razvita leta 2008, je vzpostavila programska orodja, ki omogočajo praktično izvedbo dotlej le teoretičnega koncepta pametnih pogodb (Mik, 2017: 274). Veriga podatkovnih blokov je porazdeljena podatkovna baza, v kateri se beležijo digitalne transakcije tako, da je s kriptografskimi metodami preprečeno naknadno brisanje ali spreminjanje teh zapisov. Ključno za pametne pogodbe pa je, da lahko podatkovni bloki vključujejo tudi računalniško kodo, ki jo je mogoče programirati tako, da se odzove na vnaprej definirane parametre iz blokovne verige in na verigi izvede določeno transakcijo ter njene izhodne podatke zopet zapiše v verigo.[1] Uporabniki tako lahko v obliki računalniškega algoritma v verigo blokov vključijo natančna navodila za izvršitev pametne pogodbe, npr. za prenos sredstev z enega na drug uporabniški račun, ko so za to v verigi izpolnjeni določeni pogoji (Weber, 2015: 165). Blokovnih verig je več vrst. Prav za namen omogočanja pametnih pogodb je bila zasnovana veriga Ethereum, ki vključuje programski jezik za zapis pametnih pogodb in uporabo decentraliziranih aplikacij (Mik, 2017: 276). Vsaka pametna pogodba ima na verigi Ethereum lasten javni naslov in račun, na katerem se zbirajo žetoni ether, računi uporabnikov pa lahko sprožijo izvedbo pogodbe tako, da na naslov pametne pogodbe pošljejo ustrezno zahtevo za transakcijo (De Filippi in Wright, 2018: 28). Tehnologija blockchain poleg same izpolnitve pogodbenih obveznosti zagotavlja tudi trajno dokazilo o izpolnitvi, saj so vsa dejanja znotraj verige zapisana in sledljiva.

Izraz »pametna pogodba« je lahko zavajajoč, saj računalniška koda, ki omogoča samodejno izpolnitev pogodbenih obveznosti, navadno ne pomeni tudi zapisa vseh medsebojnih obveznosti med pogodbenima strankama, ampak programski algoritem služi le kot med strankama dogovorjeni način izpolnitve pogodbe (Paulus in Matzke, 2018: 1905; Samec Berghaus in Drnovšek, 2018: 23). Načeloma bi bilo sicer mogoče v blokovno verigo zapisati tudi celotno vsebino pametne pogodbe, tako da bi vse njene določbe zabeležili v obliki programskih algoritmov. Zapis

[1] Podrobneje o tehnologiji veriženja podatkovnih blokov in njenih pravnih implikacijah glej Samec Berghaus in Drnovšek, 2018: 19–21, in De Filippi in Wright, 2018: 33–57.

pogodbe v računalniški kodi je z vidika predpisov o elektronskem poslovanju enakovreden pisni obliki, če je iz kode z uporabo računalnika naknadno mogoče prebrati vsebino pogodbe.[2] Vendar programska koda po svoji naravi ni ustrezna za zapis pomensko odprtih pogodbenih določb, ki predvidevajo npr. ravnanje stranke v razumnem roku, s skrbnostjo dobrega gospodarja, v dobri veri itd. (De Filippi in Wright, 2018: 77–78). Semantično ekvivalenco med vsebino pravnih obveznosti in računalniško kodo je mogoče doseči le pri operativnih delih pogodbe, ki jih je mogoče izraziti v obliki logičnih stavkov (če A, potem B), medtem ko neoperativnih vidikov pogodbe ni mogoče preprosto avtomatizirati (Clack, Bakshi in Braine, 2017: 5).

Ne glede na to, ali je pametna pogodba v celoti ali samo delno zapisana v računalniški kodi, je za njeno sklenitev v pravnem smislu še vedno odločilno soglasje volj dveh ali več strank (Heckelmann, 2018: 505; Samec Berghaus in Drnovšek, 2018: 22). Pogodba je dogovor med dvema ali več strankami, na podlagi katerega med njimi nastanejo pravno priznane in iztožljive pravice oz. obveznosti (Varanelli, 2014: 82).[3] Poslovno voljo za sklenitev pravno zavezujočega posla v vsakem primeru oblikujejo ljudje in ne računalniki. Zato pogodba v pravnem smislu vedno obstaja ločeno od tehničnega pojma pametne pogodbe, izvedene v obliki računalniške kode. Je pa povsem mogoče, da je soglasje za sklenitev pogodbe med strankama doseženo le v ustni obliki, medtem ko se v obliki računalniške kode zapiše le operativni del pogodbe, ki ga je mogoče avtomatizirati. Vprašanje, ali je pametna pogodba tudi pravno zavezujoča, je pomembna zato, da lahko pogodbene stranke še vedno uporabijo klasične sodne mehanizme izvršbe in reševanja sporov v primeru, če ne pride do pravilne samoizvršitve pametne pogodbe, npr. zaradi napake v računalniški kodi ali strojni opremi, ki naj bi izvršila pogodbo. To je zlasti relevantno pri pametnih pogodbah, ki se izvršijo izven verige blokov, torej v resničnem svetu, ki ni pod popolnim nadzorom omrežja (Clack, Bakshi in Braine, 2017: 4–5).

[2] Glej 13. člen Zakona o elektronskem poslovanju in elektronskem podpisu (Uradni list RS, št. 98/04 UPB, 61/06 – ZEPT in 46/14).
[3] Glej 15. in 18. člen Obligacijskega zakonika (OZ; Uradni list RS, št. 97/07 – UPB, 64/16 – odl. US in 20/18 – OROZ631).

3 Interakcija med blokovno verigo in resničnim svetom

Bistvena značilnost tehnologije blockchain je, da lahko zanesljivo potrdi resničnost dogodka znotraj blokovne verige in s tem omogoča sklepanje poslov med strankami, ki si medsebojno ne zaupajo (t. i. problem bizantinskih generalov). Zaupanje med strankami nadomesti zaupanje tehnologiji. Vendar kriptografske metode zagotavljajo le nespremenljivost tistih podatkov, ki so že v blokovni verigi, ne jamčijo pa tudi pravilnosti oz. resničnosti podatkov o zunanjih dogodkih, ki jih je v verigo zapisal zunanji agent oz. aplikacija (Mik, 2017: 277–278). Sodelovanje takšnega vmesnika je tehnično nujno v vseh primerih, ko so verižne transakcije vezane na parametre resničnega sveta. Če je npr. avtomatizirano plačilo po pametni pogodbi vezano na dostavo paketa kupcu, mora podatek o opravljeni dostavi v verigo dodati bodisi kurir, ki je dostavo opravil, bodisi sledilna naprava, ki s pomočjo signala GPS sledi lokaciji paketa. Stranki morata torej zaupati bodisi kurirju bodisi sledilni tehnologiji (Weber, 2015: 180). Blokovna veriga nikoli neposredno ne nadzoruje ali preverja resničnosti zunanjih dogodkov, saj deluje v informacijsko izoliranem okolju in ne more sama dostopati do podatkov izven svojega omrežja. Blokovni verigi so nativno vidni le podatki o poteku časa, dodajanju novih podatkovnih blokov (s transakcijskimi podatki) v verigo in prenosu digitalnih žetonov. Veriga lahko reagira le na podatke, ki so že v verigi, in neposredno izvrši le dejanja znotraj verige, zlasti prenos digitalnih žetonov. Zato je večina obstoječih pametnih pogodb sestavljena iz samodejnega plačila v kriptovaluti, ki ga sproži drug dogodek znotraj verige (Mik, 2017: 295).

Če želimo pametne pogodbe uporabljati tudi v resničnem svetu, mora biti mogoča obojestranska izmenjava podatkov med blokovno verigo in resničnim svetom. Pri pametni pogodbi, ki predvideva samodejno izvršitev plačila, ki jo sprožijo dogodki v resničnem svetu, npr. dostava fizičnega blaga, veriga potrebuje zanesljiv vir podatkov o takšnih zunanjih dogodkih. Pri pametni pogodbi, ki predvideva samodejno izpolnitev v resničnem svetu, npr. odklenitev pametne ključavnice stanovanja ali vozila na daljavo, ko je prejeto plačilo, pa mora veriga blokov posredovati ustrezen ukaz tehnični napravi, ki fizično izvrši to dejanje. V obeh položajih mora za prenos podatkov poskrbeti zaupanja vreden agent oz. aplikacija, kar je ključnega pomena za delovanje pametne pogodbe.

V nadaljevanju najprej navajam nekaj primerov pogodbenih izpolnitev, ki so lahko obojestransko izvršene znotraj blokovne verige, nato pa so analizirane težave, povezane s pogodbenimi izpolnitvami v resničnem svetu.

4 Samodejna izpolnitev pogodbe v blokovni verigi

Pametne pogodbe se sedaj največ uporabljajo pri trgovanju s kriptovalutami in elektronskimi finančnimi instrumenti, kjer se transakcija (prenos digitalnih sredstev) izvrši znotraj blokovne verige, tako da ta lahko neposredno zazna izpolnitev oz. kršitev pogodbenih obveznosti (Fries, 2018: 86). Protokoli pametne pogodbe vsebujejo pogodbene parametre ter samodejni sistem plačila, ki lahko odšteje dolgovani znesek z enega računa in ga prenese na drugega (Weber, 2015: 165). To omogoča samodejno izvršitev pogodbe z elektronskimi sredstvi: ko so znotraj verige izpolnjeni dogovorjeni pogoji, pametna pogodba sprosti plačilo, ki se prav tako izvrši znotraj verige. Če pogodba v roku ne zazna izpolnitve, lahko na enak način samodejno izplača dogovorjeno pogodbeno kazen. Plačilo se največkrat izvaja z eno od kriptovalut, saj te po svoji naravi obstajajo le znotraj blokovne verige, v obliki digitalnih žetonov. Vendar vsi digitalni žetoni ne opravljajo nalog kriptovalute, ampak lahko predstavljajo tudi vrednost konkretnega blaga ali storitve. To je značilno za začetne ponudbe kovancev (initial coin offering, ICO), katerih namenski žetoni (utility token) omogočajo imetniku dostop do blaga oz. storitev, ki jih ponuja platforma (De Filippi in Wright, 2018: 100). Čeprav so predmet posla v takšnem položaju blago ali storitve v resničnem svetu, prava interakcija med verigo blokov in resničnim svetom ni potrebna, saj avtomatizirana transakcija zadeva le prenos žetonov, ki znotraj verige predstavljajo pravico do dobrin resničnega sveta. Povezava med njimi je torej le pravna, ni pa potreben vnos zunanjih podatkov v verigo.

Na podoben način je mogoče digitalne žetone v blokovni verigi zasnovati tako, da trajno predstavljajo lastništvo fizičnih ali digitalnih dobrin, ki obstajajo izven verige. To pomeni, da žeton ni uporabljen kot plačilno sredstvo, ampak predstavlja imetnikovo izključno pravico na določenih sredstvih. Govora je o t. i. obarvanih žetonih (coloured coins) (Kempe, 2016: 19; Thomas in Huang, 2017: 20), ki bi jih bilo mogoče uporabiti npr. za pametno licenciranje avtorskih pravic na digitalnih delih (npr. digitalna glasba in računalniški programi) ali za registracijo prenosa lastništva na vrednostnih papirjih, vozilih ali nepremičninah. V tem smislu se pogosto razpravlja o možnostih za uporabo porazdeljene knjige (distributed ledger) kot alternative tradicionalnim registrom pravic. Vendar je pri tem treba razlikovati

med dvema možnima namenoma takšnega virtualnega registra, temelječega na blokovni verigi. Če je njegov namen omejen na sledenje prenosov določenih sredstev z namenom zagotoviti dokaz o transakciji oz. lastništvu, se tak porazdeljeni register lahko vzpostavi z dogovorom strank, ki se odločijo za njegovo uporabo. Še vedno pa je mogoče uporabiti drug dokaz o prenosu pravice. Če pa bi želeli zagotoviti, da je prenos digitalnega žetona priznan tudi kot edini pravno veljaven način prenosa lastništva sredstev, ki jih predstavlja žeton, bi bila za to potrebno vzpostaviti posebno zakonsko podlago, saj le zakon lahko vzpostavi pravne učinke *erga omnes* (Arrunada, 2018: 86, 96).[4]

Obarvani žetoni predstavljajo sredstva izven blokovne verige. Vendar moramo biti pravno natančnejši: žetoni predstavljajo premoženjske pravice na dobrinah, ki obstajajo v resničnem svetu, in ne teh dobrin samih. Povezava med žetoni in sredstvi, na katera se nanašajo – torej pripis premoženjskih pravic imetnikom žetonov – obstaja izključno v pravni sferi: bodisi kot pogodba med strankami bodisi kot zakonska določba. Povezava je pojmovna in ne fizična, saj prenos obarvanih kovancev ne prenese tudi fizične posesti nad sredstvi v resničnem svetu, ampak le pravice na sredstvih. Čeprav se pravni posel nanaša na predmete resničnega sveta, se njegova izpolnitev v takšnem položaju odvije v celoti znotraj blokovne verige, zato se pri takšni transakciji ne pojavijo težave v zvezi z vnašanjem dejanskih podatkov v verigo. Vendar imajo, kot rečeno, mnogi projekti blockchain večje ambicije.

5 Potrjevanje za pogodbo relevantnih dejanskih podatkov

5.1 Koncept verižnih orakljev

Pametna pogodba se lahko neposredno sklicuje na določena dejstva resničnega sveta, npr. tako, da obveznost plačila kupnine nastopi šele po fizični dostavi blaga kupcu ali da se za blago oz. storitev plača tržna cena v trenutku izpolnitve. Vsebina izpolnitve je lahko vezana tudi na druge dejanske podatke, npr. zunanjo temperaturo, valutni menjalni tečaj, izid športne tekme, porabo goriva itd. Pametna pogodba mora v takšnem primeru na nek način spremljati te parametre v resničnem svetu. Blokovna veriga je izolirana od zunanjega sveta. Če naj pametna pogodba samodejno prepozna

[4] Podrobneje o prednostih in slabostih prenosa zemljiške knjige na tehnologijo blockchain glej Thomas in Huang, 2017: 15, ter Wilsch, 2017: 761–787.

izpolnitev ene od strank (kar sproži plačilo), kršitev pogodbenih obveznosti (kar sproži pogodbeno kazen) oz. katerokoli drugo dejansko okoliščino, od katere je odvisna vsebina izpolnitve, mora biti njena računalniška koda povezana z ustreznim zunanjim podatkovnim virom (Fries, 2018: 86). Za agente, ki preverjajo podatke v resničnem svetu in jih posreduje v verigo blokov oz. za tehnično infrastrukturo, ki opravlja to nalogo, uporabljamo izraz »oraklji« (Mik, 2017: 296).

Glavna naloga verižnih orakljev je, da na varen in zanesljiv način zagotavljajo dejanske zunanje podatke, ki sprožijo izpolnitev pametne pogodbe. Tehnično je to mogoče doseči v obliki pogodbe z več podpisi (multi-signature contract), kjer mora poleg strank samih pogodbo podpisati še orakelj, ki s podpisom potrdi veljavnost zunanjih podatkov. Ko so vnaprej določeni pogoji izpolnjeni v resničnem svetu, orakelj podpiše transakcijo s svojim zasebnim ključem in tako sproži njeno izvršitev (Hurr 2016: 24–25). Pri pametnih pogodbah na platformi Ethereum pa lahko računalniška koda pametne pogodbe tudi sama preveri pogoje in sproži transakcijo v skladu s pravili odobritvenega algoritma. To pomeni da je orakljeva vloga le posredovanje zunanjih podatkov v blokovno verigo, medtem ko njegov podpis ni potreben (Bertani, 2016).

Drugače kot verige blokov oraklji niso decentralizirani, zato tehnologija blockchain ne zagotavlja pravilnosti podatkov, ki jih zagotovijo. Stranke morajo torej oraklju zaupati in se zanesti na to, da bo svojo nalogo opravil korektno in neodvisno (Mik, 2017: 296). Če posameznemu agentu ne zaupajo dovolj, lahko v pogodbo vključijo tudi več orakljev, tako da se transakcija znotraj verige izvrši šele, ko vsi oraklji dodajo svoj podpis, kar zmanjša možnost goljufije (Bertani, 2016). V vsakem primeru je priporočljivo, da se stranke pametne pogodbe vnaprej dogovorijo o tem, ali je orakelj edini dopusten dokaz o izpolnitvi pogodbenih obveznosti[5] oz. ali je v primeru spora dopustna tudi uporaba drugih dokaznih sredstev (Fries, 2018: 90).

Čeprav je temeljna vloga vseh orakljev enaka, se način njihovega delovanja lahko bistveno razlikuje. V tehničnem smislu lahko ločimo med tremi tipi orakljev:

- programski oraklji,
- strojni oraklji in

[5] V takšnem primeru pogodba velja za izpolnjeno šele, ko izpolnitev potrdi orakelj, tako da je orakljeva potrditev pravzaprav del dogovorjenega izpolnitvenega ravnanja.

– človeški oraklji.

Način orakljevega delovanja pri izvršitvi pametne pogodbe definira tudi njegov pravni položaj znotraj pravnega posla.

5.2 Programski oraklji

Podatki o vrstah dejanskih dogodkov in stanj resničnega sveta, ki so lahko relevantni za pametno pogodbo, so že dostopni na internetu v različnih javnih bazah podatkov. Spletne strani javnih meteoroloških služb objavljajo vremenske podatke za posamezne kraje, finančni mediji zagotavljajo podatke o borzni ceni vrednostnih papirjev, nafte, zlata ter o menjalnih tečajih, spletne strani transportnih podjetij objavljajo podatke o prihodih in zamudah v javnem prevozu, športne organizacije objavljajo rezultate tekem itd. Če stranke zaupajo takšnemu javno dostopnemu viru podatkov, je za njegovo uporabo v pametni pogodbi potreben le računalniški program, ki potrebni podatek izvleče iz podatkovnega vira in ga potisne v blokovno verigo, kjer ga uporabi decentralizirana aplikacija pametne pogodbe. Takšnim algoritmom rečemo programski oraklji (Rabesandratana in Bacca 2018: 91). Primera programskih orakljev sta spletni storitvi Oraclize[6] in Reality Keys,[7] ki že ponujata samodejno preverjanje kateregakoli podatka na podlagi javno dostopnih programskih vmesnikov (API).

Obstaja več kriptografskih metod, s katerimi programski orakelj lahko potrdi izvor podatkov in dokaže, da so podatki, pridobljeni iz izvirnega vira podatkov, resnični in nespremenjeni, npr. dokazili TLSnotary ali Oraclize, ki spremljata posredovane podatke. Ta vrsta programskih orakljev je razmeroma preprosto izvedljiva. Vendar morajo stranke zaupati tako viru podatkov kot samemu oraklju, saj so podatki lahko kompromitirani na obeh mestih. Tehnologija blockchain zagotavlja le nespremenljivost podatkov po tem, ko so bili vključeni v verigo blokov. Možna rešitev je uporaba omrežja programskih orakljev, ki pridobijo podatke iz več neodvisnih podatkovnih virov, pri čemer mora veljavnost parametra resničnega sveta za namene pogodbe potrditi več orakljev (Mik, 2017: 297). To se lahko razvije v kompleksne mehanizme soglasja, temelječe na ugledu, ki bi v končni fazi lahko sestavljali decentralizirane programske oraklje (Larchevêque, 2016).

[6] http://www.oraclize.it/ (dostop: 5. 12. 2018).
[7] https://www.realitykeys.com/ (dostop: 5. 12. 2018).

5.3 Strojni oraklji

Največ podatkov resničnega sveta, ki so lahko relevantni za izpolnitev pametne pogodbe, ni javno dostopnih in jih ni mogoče samodejno prevzeti iz spletnih podatkovnih virov. To velja zlasti za podatke o posameznih izpolnitvah, npr. ali je bilo konkretno blago dobavljeno v skladu s pogodbo oz. ali je bila storitev opravljena tako, kot je bilo dogovorjeno. Takšnih dejstev ni mogoče preveriti prek javnih spletnih virov ali z metodo soglasja orakljev, saj je treba dejstva preveriti (ali izmeriti) lokalno, na mestu izpolnitve, in to pogosto v realnem času (Rabesandratana in Bacca, 2018: 92). Za zagotovitev samodejnega potrjevanja takih dejstev je treba vzpostaviti ustrezno tehnološko infrastrukturo za spremljanje določenih dogodkov ali stanj resničnega sveta. Sledenje blaga v dobavni verigi je npr. mogoče doseči z opremljanjem vseh paketov z oznakami RFID in uporabo senzorjev na vratih skladišč in transportnih vozil ali pa z opremljanjem vseh paketov z GPS sledilnimi enotami. Dostava paketa na določeno lokacijo lahko nato sproži samodejno plačilo v skladu s pametno pogodbo (Weber, 2015: 166). Pametni električni števci lahko brezžično pošiljajo odčitke vodnih števcev komunalnemu podjetju in mu omogočajo, da vsak mesec izda natančen račun glede na porabo.

Za takšno nadzorno tehnologijo, ki pošilja podatke pametnim pogodbam na blokovni verigi se uporablja izraz strojni oraklji (hardware oracles), včasih pa tudi strojne Pitije (hardware Pythias) (Larchevêque, 2016). Mogoče bi jih bilo uporabiti tudi za precej naprednejše spremljanje parametrov resničnega sveta, kot je to običajno oz. sploh možno pri klasičnih pogodbah. Pri pametnem avtomobilskem zavarovanju bi npr. senzorji v avtu spremljali voznikovo ravnanje v prometu in prilagodili premijo zaznanim tveganjem, tako da bi bili vozniki nagrajeni za dobro obnašanje na cesti, vozniki s prekrški pa bi izgubili bonus (Rosenberger, 2018: 98). Z razvojem izdelkov, ki vsebujejo z internetom povezane senzorje – t. i. interneta stvari – naj bi sprotno pridobivanje podatkov o trenutni lokaciji in stanju takšnih objektov v resničnem svetu postalo bolj dostopno (Mik, 2017: 297–298). Stranke pametne pogodbe lahko potrebno tehnično infrastrukturo vzpostavijo same ali pa se pri tem zanašajo na druge ponudnike, ki takšno infrastrukturo že imajo, npr. špedicijska in logistična podjetja. Za varno poročanje o zaznavi senzorja mora imeti vsaka naprava zasebni ključ za kriptografsko preverjanje pristnosti meritev senzorja in ukrep proti nedovoljenemu spreminjanju, ki v primeru kakršnega koli poskusa manipulacije napravo takoj onemogoči z brisanjem zasebnih ključev (Rabesandratana in Bacca, 2018: 92).

5.4 Človeški oraklji

Mnoge vrste pogodbenih izpolnitev niso računalniško preverljive niti programsko niti strojno, ker jih ni mogoče izmeriti z objektivnimi merili. Senzorji lahko nadzirajo lokacijo, število ali težo dobavljenega blaga, medtem ko je za preverjanje kakovosti in videza izdelkov navadno še vedno potreben človek. Seveda bo tehnični napredek senzorjev in tehnologije prepoznavanja slik verjetno povečal število kazalnikov kakovosti, ki jih bo mogoče samodejno izmeriti, zlasti pri standardiziranem blagu ali storitvah. Toda ljudje so primernejši za ocenjevanje obveznosti, ki jih ni mogoče zlahka pretvoriti v pametno pogodbo, ker zahtevajo subjektivno vrednotenje dogodkov iz resničnega sveta (De Filippi in Wright, 2018: 75). Zavarovalnice se bodo verjetno še naprej zanašale na človeške ocenjevalce škod, namesto da bi vzpostavile zapleten sistem senzorjev, saj lahko ljudje pregledajo številne vrste škod in hkrati lažje ocenijo utemeljenost zahtevka oz. posumijo, da gre za zavarovalno goljufijo. Prednost človeškega ocenjevanja je očitna tudi v primerih, ko je treba pogodbeno izpolnitev ovrednotiti celovito in ne le z meritvijo posameznih parametrov, npr. kadar gre za standarde, kot sta dobra vera ali skrbnost dobrega gospodarja (Mik, 2017: 298). Za ocenjevanje izpolnitve takšnih pogodbenih obveznosti bi računalniški programi potrebovali visoko raven splošne umetne inteligence (Abramowicz, 2016: 362).

Če so pri redni izpolnitvi pametne pogodbe udeleženi človeški oraklji (in ne sodelujejo le kot arbitri v primeru spora), potem pogodbena izpolnitev v resnici ni povsem avtomatizirana. Kljub temu si lahko zamislimo, da bi stranke še vedno izbrale obliko pametne pogodbe zato, da bi z njo zagotovile vzajemno izpolnitev – npr. plačilo v zameno za dobavo blaga. Pametna pogodba z več podpisi, kjer je avtomatizirano plačilo s kriptovaluto, ki pa se izvrši šele, ko dobavljeno blago osebno pregleda v pogodbi določeni agent (človeški orakelj), doseže ekonomsko podoben učinek kot prodaja blaga z dokumentarnim akreditivom, vendar brez sodelovanja banke, kar lahko bistveno zmanjša transakcijske stroške. Prednost človeških orakljev je tudi prilagodljivost njihove storitve potrebam posamezne transakcije, medtem ko programski in strojni oraklji opravljajo le standardizirana, vnaprej opredeljena opravila.

Uporaba človeških orakljev v povezavi s pametnimi pogodbami je doslej predvsem teoretični koncept, ki pa bi ga bilo razmeroma preprosto izvesti v praksi, saj različne službe, ki se ukvarjajo s potrjevanjem dobave in preverjanjem kakovosti blaga, že obstajajo. Ladijski prevoznik npr. s pomorsko nakladnico potrdi prejem tovora za prevoz, in takšno nakladnico je mogoče izdati tudi v elektronski obliki, primerni za uporabo v blokovni verigi (Van Maanen in Regtien, 2018). Prej omenjeni ponudnik programskih orakljev Reality Keys ponuja tudi človeško preverjanje podatkov za pametne pogodbe, vendar je storitev zaenkrat omejena na dodatno preverjanje, da so bili podatki samodejno pravilno prevzeti iz ustreznega programskega vmesnika, tako da pri tem ne gre za pravega človeškega oraklja. Zanimiva je tudi zamisel množičnega oraklja RealityCheck,[8] ki mu lahko kdorkoli zastavi vprašanje in prav tako lahko kdorkoli odgovori na vprašanje, pri čemer pa so uporabniki, ki odgovorijo pravilno, za odgovor nagrajeni, uporabniki, ki odgovorijo napačno, pa kaznovani. Nagrade se financirajo iz plačila zastavljavcev vprašanj in iz kazni, plačanih za napačne odgovore. Če ni soglasja o pravilnem odgovoru, se lahko angažira še arbitra, čigar odločitev je končna (Edgar, 2017). Takšna decentralizirana orakeljska storitev je lahko zanesljivejša od posameznega oraklja, vendar ni primerna za pogodbe z visoko vrednostjo, saj je množično odgovarjanje na vprašanja mogoče manipulirati.

6 Pravni položaj orakljev

6.1 Splošno

Medtem ko nekateri programski oraklji že delujejo, strojni in človeški oraklji trenutno obstajajo bolj kot koncept, ne pa tudi kot mehanizem, ki se uporablja v praksi, četudi je nedvomno tehnično izvedljiv. Zato pravna analiza njihovega položaja ne more temeljiti na preučevanju dejansko vzpostavljenih pogodbenih razmerij oz. z njimi povezane sodne prakse. Vendarle pa je mogoče izpostaviti nekatera glavna vprašanja v razmerju med strankami pametne pogodbe in izvajalcem orakeljske storitve, ki jih je smiselno pravno urediti. Pri tem je treba razlikovati med dvema, sicer medsebojno povezanima, pogodbenima razmerjema:

- razmerje med strankami pametne pogodbe na eni strani in orakljem na drugi strani;

[8] https://realitykeys.github.io/realitycheck/ (dostop: 5. 12. 2018)

- medsebojno razmerje med strankami pametne pogodbe v zvezi z orakljevo vlogo pri izpolnitvi pametne pogodbe.

Velja opozoriti, da če je pametna pogodba v tehničnem smislu oblikovana v obliki transakcije z več podpisi, ki jo mora za izvršitev podpisati eden ali več orakljev, to še ne pomeni večstranske pogodbe. Oraklji namreč niso stranke pri sami pametni pogodbe, ampak le pomočniki pri njeni izpolnitvi. Medtem kot strankin podpis izraža njeno soglasje za sklenitev pogodbe,[9] je orakljev podpis tehnične narave in potrjuje le, da so v resničnem svetu izpolnjeni pogoji, za spremljanje katerih je bil orakelj pooblaščen. Orakljev podpis je torej že element izpolnitve pogodbe. Pravila opravljanja orakeljske storitve pa so predmet ločenega pogodbenega razmerja med orakljem in strankami pametne pogodbe.

6.2 Razmerje med strankami pametne pogodbe in orakljem

Za uporabo samoizvršljive pametne pogodbe, pri kateri je orakelj zadolžen za preverjanje dejanskih pogojev za izpolnitev pogodbenih obveznosti v resničnem svetu, bi se stranke navadno odločile v položaju, ko ne zaupajo povsem, da bo nasprotna stranka prostovoljno izpolnila svoje pogodbene obveznosti. Ker je pri takšni rešitvi orakelj v položaju, kjer je mogoča manipulacija z zunanjimi podatki, mora biti v razmerju do obeh strank neodvisen in nepristranski (Cieplak in Leefatt, 2017: 424).

Obstoječi programski oraklji so na voljo kot brezplačne ali nizkocenovne spletne storitve in, podobno kot pri mnogih drugih brezplačnih spletnih storitvah, (kvazi)pogodbeno razmerje med ponudnikom in uporabniki storitve ni jasno definirano. Če si pogledamo pogoje poslovanja spletnih storitev Oraclize[10] in Reality Keys,[11] opazimo, da ti ne posvečajo pozornosti pravnemu položaju oraklja v razmerju do strank pametne pogodbe. Orakljeva nepristranost ni izrecno zagotovljena, morda zaradi pričakovanja, da je že tehnološka rešitev sama dovolj nevtralna, saj le prevzame podatke iz zunanjega podatkovnega vira in jih posreduje v blokovno verigo, ne da bi jih lahko spremenila po navodilu stranke, ki je angažirala orakljeve storitve. Pri storitvi, ki se opravlja zastonj ali financira le prek oglaševanja,

[9] Prim. 18. in 57. člen OZ.
[10] http://docs.oraclize.it/(dostop: 5. 12. 2018).
[11] https://www.realitykeys.com/legal (dostop: 5. 12. 2018).

najbrž ne moremo pričakovati, da bo ponudnik prevzel še kakršnekoli dodatne obveznosti do uporabnikov storitve.

V primeru uporabe orakeljskih storitev za sprožitev izpolnitve kakršnegakoli pravnega posla večje vrednosti pa lahko pričakujemo, da bo pri tem šlo za plačljivo storitev, urejeno s tri- ali večstransko pogodbo med strankami pametne pogodbe in orakljem. Pogodba o opravljanju orakeljske storitve bi morala določiti obveznost orakljeve nepristranosti in enake pogodbene lojalnosti obema strankama. Opredeliti bi morala, kaj se šteje za nedopustno navzkrižje interesov in izrecno prepovedati sprejemanje navodil od posamezne stranke ali celo ločeno komuniciranje s posamezno stranko. V tem pogledu bi orakljev položaj lahko primerjali s položajem arbitra v arbitražnem postopku. Pri storitvah programskih orakljev zahteva po nevtralnem položaju oraklja pomeni predvsem zavezo, da verodostojno prenese relevantne podatke iz spletnega vira v blokovno verigo. Storitve strojnih in človeških orakljev pa bodo nujno manj standardizirane in bolj prilagojene posebnim značilnostim posamezne transakcije. V takšnem primeru bi stranke morale z orakljem skleniti posebno pogodbo o orakeljski storitvi, s katero bi se natančno opredelile orakljeve naloge preverjanja dejstev v zvezi z določene pametno pogodbo: katere parametre mora orakelj preveriti v resničnem svetu, katero metodo naj za to uporabi in pod katerimi pogoji naj podpiše pametno pogodbo, da sproži njeno samodejno izvršitev. Za zagotovitev orakljeve neodvisnosti je smiselno določiti tudi, da orakelj ne sme upoštevati posebnih navodil, ki bi mu jih dala samo ena od strank in da morata kakršnekoli spremembe orakljevih nalog odobriti obe stranki pametne pogodbe.

Glede zanesljivosti orakeljskih storitev velja omeniti, da pogoji poslovanja storitve Reality Keys izrecno izključujejo kakršnokoli jamstvo pravilnosti ali točnosti odgovorov, ki jih zagotavlja orakelj. Uporabnikom se svetuje, naj preverijo vse informacije, ki jih nudi storitev, in sprejmejo ustrezne ukrepe za preprečitev izgube ali škode v primeru, da so podatki napačni. Takšna določba je razumljiva v pogojih brezplačne storitve spletnega oraklja, ne bi pa bila sprejemljiva v pogojih plačljivih orakeljskih storitev. Orakelj bi moral zagotavljati vsaj, da so uporabljeni najsodobnejši tehnični ukrepi za pravilno pridobitev ustreznih podatkov iz dogovorjenega vira podatkov in da so ti podatki posredovani v blokovno verigo brez sprememb ali možnosti zunanjih motenj. Pri strojnih orakljih bi pogodba morala določiti tudi ponudnikove obveznosti glede namestitve in vzdrževanja senzorjev in druge tehnične opreme, potrebne za merjenje parametrov resničnega sveta. Človeški

oraklji pa bi se morali zavezati, da bo zahtevano oceno dogodkov v resničnem svetu izvedlo ustrezno usposobljeno osebje ter da bo naloga opravljena z najboljšimi prizadevanji in skrbnostjo dobrega strokovnjaka. Ponudnik plačljivih orakeljskih storitev bi moral strankam jamčiti tudi zanesljivost zagotavljanja storitev v predvidenem obdobju, tako da se tok podatkov iz resničnega sveta v blokovno verigo ne ustavi zaradi tehnične napake ali ker bi orakelj prenehal opravljati svojo storitev. Orakelj bi moral zagotavljati minimalne standarde dosegljivosti storitve (Cieplak in Leefatt, 2017: 424).

Ironično, zaradi številnih odprtih, nebinarnih določb, ki opredeljujejo orakljeve naloge, pogodba o zagotavljanju orakeljskih storitev najbrž nikoli ne bo sklenjena v obliki pametne pogodbe, saj takšnih določb ni mogoče preprosto preliti v računalniško kodo.

6.3 Razmerje med strankami pogodbe glede orakljevih storitev

Računalniška koda pametne pogodbe opredeljuje orakljevo vlogo pri samodejni izvršitvi pogodbenih obveznosti, in sicer dodajanje podpisa, ko so izpolnjeni določeni pogoji, oz. dodajanje specifičnih podatkov o zunanjih dogodkih v blokovno verigo. Pametna pogodba hkrati določa pravne posledice orakljeve verifikacije nekaterih dejstev in ustvarja tehnična pravila za samodejno izpolnitev pogodbenih obveznosti, ki jo sproži ta verifikacija. Vendar je smotrno, da se stranke pametne pogodbe dogovorijo še, kaj se zgodi, če bodisi orakljeva storitev bodisi podatkovni vir, na katerega je vezana, preneha delovati (Weber 2015: 173). Tehnične težave lahko preprečijo samodejno izvršitev pametne pogodbe, ki pa – če ni dogovorjeno drugače – stranke še naprej zavezuje. Pogodba bi zato morala določiti, kako lahko stranke na drug način dokažejo, da so pogoji za plačilo izpolnjeni. Plačilo se lahko nato izvede »ročno«, četudi v obliki kriptovalute. V primerih, ko bi orakelj moral potrditi bolj nevsakdanja dejstva, za preverjanje katerih ne obstaja alternativni vir podatkov oz. dokaz, bi lahko pogodba pooblastila tretjo stranko, da odloči, kdo je upravičen do denarja, ali pa določila, da se pogodba v takšnem položaju razdre (Weber, 2015: 166–167). V poštev pride tudi uporaba določb 116. člena OZ o naknadni nemožnosti izpolnitve pogodbe, za katero ne odgovarja nobena stranka, zaradi česar ugasneta obveznosti obeh pogodbenih strank.

Drugo vprašanje je, kaj se zgodi, če tehnična napaka, npr. napačen odčitek parametrov, ki jih merijo strojni senzorji, povzroči samodejno izpolnitev nečesa, kar ni bilo dolgovano. Če sta se obe stranki zanašali na napačne podatke iz resničnega sveta, ne da bi vedeli za napako, bi lahko govorili o obojestranski zmoti. V vsakem primeru izpolnitev pogodbe, ki temelji na napačnih dejanskih podatkih resničnega sveta, ne ustreza pravicam in obveznostim strank, ki sledijo iz pametne pogodbe kot pravnega posla, ne glede na to, da je takšna izpolnitev skladna s tehničnim algoritmom pametne pogodbe. V takšnem primeru je treba uporabiti splošna pravila obligacijskega prava o neupravičeni obogatitvi in vrniti plačilo tistega, kar ni bilo dolgovano (190. člen OZ). To ponovno kaže, zakaj je pomembno, da je pametna pogodba tudi pravno zavezujoča in se za svojo izvršitev ne zanaša samo na tehnologijo.

Kjer se strojni senzorji uporabljajo za spremljanje izpolnjevanja pogodbenih obveznosti, se bo verjetno pogosto zgodilo, da bo za namestitev in vzdrževanje potrebne infrastrukture poskrbela ena od pogodbenih strank in ne od strank neodvisni agent. Prevozna podjetja imajo npr. že vzpostavljeno tehnično infrastrukturo za sledenje pošiljkam, ki jo je mogoče prek spleta brez večjih težav povezati z blokovno verigo. Prevoznik lahko s to opremo deluje kot orakelj pri pametni prodajni pogodbi, kjer bo kot tretja stranka potrdil izpolnitev prodajalčeve obveznosti glede izročitve blaga. Če pa je v obliki pametne pogodbe sklenjena prevozna pogodba, tako da predvideva samodejno plačilo, ko blago prispe v namembni kraj, bo podatek o izpolnitvi prevoznikove pogodbene obveznosti zagotovila oprema ene od strank pametne pogodbe in ne od strank neodvisnega agenta. V tehničnem smislu pa je takšna oprema še vedno strojni orakelj, ki potrjuje dejstva resničnega sveta in jih posreduje blokovni verigi. Če bi stranka manipulirala z meritvami svojih naprav, da bi lažno prikazala pravilno izpolnitev pogodbenih obveznosti, bi šlo seveda za prevaro in bi bila nasprotna stranka upravičena zahtevati vračilo svoje izpolnitve. V izogib nesporazumom glede narave in namena tehnične infrastrukture, ki jo zagotavlja ena od strank, bi morali stranki pametne pogodbe izrecno določiti jamstva glede nemotenega delovanja opreme brez posegov stranke. Nasprotna stranka bi morala imeti možnost, da v primeru dvoma zahteva naknadno preveritev izvedene meritve.

7 Samodejna izpolnitev pametne pogodbe v resničnem svetu

Doslej smo obravnavali samo vhodne oraklje, katerih naloga je posredovanje zunanjih podatkov v blokovno verigo. Obstajajo pa tudi izhodni oraklji, ki omogočajo blokovni verigi, da poseduje podatke v resnični svet. To je važno, kadar stranki želita doseči samodejno izvršitev pogodbe izven podatkovne verige. *Szabo* je že leta 1996 razpravljal o možnosti razširitve zamisli pametnih pogodb na t. i. pametno premoženje (smart property), ki bi ga ustvarili z vgnezdenjem pametnih pogodb v fizične predmete. Vgnezdeni protokoli bi samodejno predali možnost uporabe tega premoženja stranki, ki je do tega upravičena na podlagi pogodbe (Szabo, 1996). To zamisel skuša danes uresničiti zagonsko podjetje Slock.it,[12] ki razvija pametne ključavnice, ki lahko samodejno odklenejo oz. zaklenejo vrata z internetom povezanih vozil ali stanovanj, ko je bilo prejeto plačilo za njihovo uporabo. To bi lahko zelo olajšalo oddajanje in najemanje z internetom povezanih stvari brez posrednikov, kar je zanimivo zlasti z vidika delitvene ekonomije (Hurr, 2016: 32).

Koncept interneta stvari predvideva, da bodo poleg pametnih ključavnic z internetom kmalu povezane tudi druge vsakodnevne naprave v naših domovih, npr. termostati, svetila in senčila, kar bi pametnim pogodbam lahko širše omogočilo upravljanje naprav in sprožanje dogodkov tudi v resničnem svetu. To pa spet terja izmenjavo podatkov med blokovno verigo in resničnim svetom, in sicer mora pametna pogodba posredovati ukaze pametnim napravam in od njih prejeti odziv, ki potrdi uspešno ali neuspešno izvedbo ukaza. Naloga izhodnega oraklja je opazovanje stanja blokovne verige in posredovanje navodil pametne pogodbe pametnim napravam, naj opravijo dejanja, ki so relevantna za izpolnitev pogodbe (Arrunada, 2018: 84). Vendar je treba upoštevati, da je takšno avtomatizirano upravljanje pametnega premoženja primerno zlasti za izpolnitev lastnikove obveznosti, da premoženje preda v uporabo nasprotni stranki, ne pa tudi za odvzem možnosti uporabe nekooperativni stranki. Objekti in dejanja v fizičnem svetu namreč nikoli ne morejo biti pod popolnim nadzorom omrežja (Clack, Bakshi in Braine, 2017: 4). Če npr. najemnik noče izprazniti stanovanja in novim stanovalcem preprečuje vstop ali če leasingojemalec noče vrniti vozila leasingodajalcu, zgolj samodejna onesposobitev njegovih ključev na daljavo ne zadošča, ampak se mora lastnik zanesti na tradicionalne sodne mehanizme varstva posesti in izvršbe.

[12] https://slock.it/ (dostop: 5. 12. 2018).

Po drugi strani tehnologija blockchain prav tako ne zagotavlja popolnega varstva najemniku stanovanja ali vozila, saj lahko lastnik še vedno zamenja pametno ključavnico in najemniku tako prepreči uporabo stvari, do katere je upravičen. Omejena uporabnost pametnih ključavnic je eden od razlogov, zaradi katerih lahko domnevamo, da neodvisnost izhodnih orakljev ne bo tako pomembna kot pri vhodnih orakljih, o katerih smo razpravljali zgoraj. Drug razlog za to je, da so pametne ključavnice v predstavljenih primerih uporabljene predvsem kot pomoč najemodajalcu pri izpolnitvi njegovih pogodbenih obveznosti, ne pa za potrjevanje izpolnitve s strani pogodbene stranke. Ker predmet pogodbe ni prenos lastninske pravice, ampak samo dovolitev začasne uporabe predmetov, najete stvari ostanejo v posredni posesti najemodajalca (drugi odstavek 24. člena Stvarnopravnega zakonika;[13] SPZ). Zato bi lahko najemodajalec opremil svojo lastnino s pametnimi ključavnicami in sam upravljal orakeljsko programsko opremo ali pa to prepustil tretjemu ponudniku storitev, ki bi potem deloval kot najemodajalčev pomočnik pri izpolnitvi pogodbene obveznosti in ne kot neodvisna tretja stranka. Seveda je to odvisno tudi od dogovora strank o tem, kako je treba izvajati pametno pogodbo.

Že obstoječa pametna tehnologija so pametni števci za električno energijo ali vodo, ki se povezujejo z internetom in komunalnemu podjetju v realnem času sporočajo meritve porabe, obvestila o prekinitvah napajanja, podatke o kakovosti dobave električne energije itd. S tem nedvomno lahko služijo tudi kot vhodni oraklji pri pametnih pogodbah, lahko pa bi jih uporabili tudi kot izhodne oraklje, če bi jih povezali s pametnimi ventili in programirali tako, da samodejno prekinejo oskrbo z električno energijo ali vodo, če plačilo ni izvedeno pravočasno. V takšnem položaju bi pametna pogodba prek oraklja hkrati nadzirala izvrševanje pogodbenih obveznosti in izvrševala pogodbene sankcije za neizpolnitev obveznosti (Paulus in Matzke, 2018: 1906). Vendar bi bil ravno na področju dobave vode in električne energije samodejni odklop lahko pravno nedopusten, zlasti v razmerju do potrošnika, saj bi praktično odpravil sodni nadzor nad strogim ukrepom in v praksi prevalil breme dokazovanja neupravičenosti odklopa na potrošnika (Ibidem*:* 1910). Energetski zakon (EZ-1)[14] v drugem odstavku 51. člena npr. določa, da distribucijski operater ne sme ranljivemu odjemalcu odklopiti elektrike oz. odjema omejiti pod količino oz. moč, ki je glede na okoliščine (letni čas, temperaturne razmere, kraj prebivanja, zdravstveno stanje in druge podobne okoliščine) nujno potrebna, da ne

[13] Uradni list RS, št. 87/02 in 91/13.
[14] Uradni list RS, št. 17/14 in 81/15.

pride do ogrožanja življenja in zdravja odjemalca ter oseb, ki z njim prebivajo. Podobno določa prvi odstavek 176. člena EZ-1 glede prekinitve oskrbe ranljivih odjemalcev z zemeljskim plinom. V takšnih položajih uporaba pametne pogodbe torej ne bi bila dopustna.

8 Zaključek

Sodelovanje verižnega oraklja je tehnično nujno pri vseh pametnih pogodbah, ki za svojo samodejno izpolnitev potrebujejo dostop do podatkov izven blokovne verige. Orakljeva vloga je najpreprostejša, kadar v blokovno verigo le posreduje podatke iz javno dostopnega internetnega vira, pogodbene izpolnitve pa se izvršijo znotraj blokovne verige, npr. s prenosom digitalnih žetonov. Stranki pametne pogodbe se morata pri tem zanesti samo na verodostojnost podatkovnega vira in zaupati oraklju, da bo korektno prenesel prave podatke iz vira. Glede tega se lahko zaneseta na splošne pogoje opravljanja storitve spletnega oraklja ali pa s ponudnikom orakeljske storitve skleneta posebno tristransko pogodbo. Posebna pogodbena ureditev razmerij med strankami pametne pogodbe in orakljem pa bo pomembnejša pri strojnih in človeških orakljih, katerih naloga je nadzorovanje, potrjevanje ali sprožanje pogodbenih izpolnitev v resničnem svetu. Pri teh nalogah je možnost napak ali zlorab precej večja, zato stranki ne bi smeli posvečati pozornosti samo računalniški kodi, v kateri je zapisana pametna pogodba, ampak tudi pravnim pogojem, ki urejajo njuno razmerje do oraklja in medsebojno razmerje v zvezi z orakljem. Tristranska pogodba med strankama pametne pogodbe in orakljem bi morala zagotavljati orakljevo neodvisnost in nepristranost v razmerju do obeh strank ter njegovo zavezo k opravljanju storitve z najvišjo strokovno skrbnostjo. Že v pametni pogodbi pa bi morali stranki predvideti, kako bosta ravnali v primeru, če orakeljska storitev odpove iz tehničnih ali drugih razlogov. Ker so tehnične težave vedno mogoče, je bistveno, da se pametne pogodbe, ki temeljijo na izmenjavi podatkov z resničnim svetom, nikoli ne zanašajo izključno na računalniško kodo, ampak da razmerje med strankami uredijo tudi s pravnega vidika in tako v primeru zapletov omogočijo reševanje spora s sodnimi mehanizmi.

Uporaba programskih orakljev za pridobivanje podatkov iz zanesljivih spletnih podatkovnih baz je privlačna, če zmanjša potrebni čas in stroške izpolnitve pogodbenih obveznosti, vendar pride v poštev le za razmeroma preproste in standardizirane transakcije. S pomočjo strojnih in človeških orakljev je mogoče v obliko pametne pogodbe pretvoriti tudi mnogo bolj zapletena poslovna razmerja,

vendar to terja tudi natančno pogodbeno ureditev orakljevega položaja za vsak primer posebej. S kompleksno orakeljsko storitvijo so gotovo povezani tudi višji stroški. Glede na to se zdi verjetno, da bodo strojni, še posebej pa človeški oraklji ostali mnogo redkejši od preprostih programskih orakljev. Posledično se bo zagotavljanje orakeljskih storitev verjetno razvilo predvsem za standardizirane transakcije, kjer je treba preveriti določen niz parametrov resničnega sveta. Skupaj s standardizirano orakeljsko storitvijo pa se bodo razvili tudi standardizirani pogodbeni pogoji, v skladu s katerimi se bo storitev opravljala.

Literatura

Abramowicz, M. (2016) Cryptocurrency-Based Law, Arizona Law Review, 58(2), strani 359–420.

Arrunada, B. (2018) Blockchain's Struggle to Deliver Impersonal Exchange, Minnesota Journal of Law, Science & Technology, 19(1), strani 55–105.

Bertani, T. (2016) Understanding oracles, Oraclize Blog, 18 February 2016, https://blog.oraclize.it/understanding-oracles-99055c9c9f7b (uporabljeno 3. 12. 2018).

Cieplak, J., Leefatt, S. (2017) Smart Contracts: A Smart Way to Automate Performance, Georgetown Law Technology Review, 1(2), strani 417–427.

Clack, C.D., Bakshi, V.A., Braine, L. (2017) Smart Contract Templates: foundations, design landscape and research directions, v3, https://arxiv.org/abs/1608.00771v3 (uporabljeno 3. 12. 2018).

De Filippi, P., Wright, A. (2018) Blockchain and the Law: The Rule of Code (Cambridge, Massachusetts: Harvard University Press).

Fries, M. (2018) Smart Contracts: Brauchen schlaue Verträge noch Anwälte? Anwaltsblatt, 68(2), stani 86–90.

Heckelmann, M. (2018) Zulässigkeit und Handhabung von Smart Contracts, Neue Juristische Wochenschrift, 71(8), strani 504–510.

Hurr, E. (2016) Smart Contracts und ihre Verwendungsmöglichkeiten im Finanzsektor, Deutsche finance- und versicherungswirtschaftliche Studienreihe Nr. 4 (München: GRIN Verlag).

Kempe, M. (2016) The Land Registry in the Blockchain (Stockholm: Lantmäteriet, Telia, ChromaWay, Kairos Future).

Larchevêque, E. (2016) Hardware Pythias: bridging the Real World to the Blockchain, Ledger, 31 August 2016, https://www.ledger.fr/2016/08/31/hardware-pythias-bridging-the-real-world-to-the-blockchain (uporabljeno 3. 12. 2018).

Mik, E. (2017) Smart contracts: terminology, technical limitations and real world complexity, Law, Innovation and Technology, 9(2), strani 269–300.

Paulus C.G., Matzke, R. (2018) Smart Contracts und Smart Meter – Versorgungssperre per Fernzugriff, Neue Juristische Wochenschrift, 71(27), strani 1905–1911.

Rabesandratana, V., Bacca, N. (2018) L'Oracle hardware : la couche de confiance entre les blockchains et le monde physique, Réalités Industrielles, août 2017, strani 91-93.

Rosenberger, P. (2018) Bitcoin und Blockchain: Vom Scheitern einer Ideologie und dem Erfolg einer revolutionären Technik (Berlin: Springer Vieweg).

Samec Berghaus, N., Drnovšek, K. (2018) Iluzija pojma pametne pogodbe. V: Repas, M. (ur.), Pravo in ekonomija: Digitalno gospodarstvo (Maribor: Univerzitetna založba UM).

Szabo, N. (1996) Smart Contracts: Building Blocks for Digital Markets, Extropy, The Journal of Transhumanist Thought, 16: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html (uporabljeno 3. 12. 2018).

Thomas, R., Huang, C. (2017) Blockchain, the Borg collective and digitalisation of land registries, The Conveyancer and Property Lawyer, 2017(1), strani 14–25.
Van Maanen, M., Regtien, I. (2018) E-bills of lading, Lexology, 20 April 2018, https://www.lexology.com/library/detail.aspx?g=453d225f-ca8b-404f-9b39-f39f4f0a7b90 (uporabljeno 3. 12. 2018).
Varanelli, L. (2014) Pogodbeno pravo I (Ljubljana: GV Založba).
Weber, R.H. (2016) Contractual Duties and Allocation of Liability in Automated Digital Contracts. V: Schulze, R., Staudenmayer, D. (ur.). Digital Revolution: Challenges for Contract Law in Practice (Baden Baden: Hart, Nomos).
Wilsch, H., (2017) Die Blockchain-Technologie aus der Sicht der deutschen Grundbuchrechts, Deutsche Notar-Zeitschrift», 2017(10), strani 761–787.

O avtorju

Doc. dr. Matija Damjan je zaposlen na Inštitutu za primerjalno pravo pri Pravni fakulteti Univerze v Ljubljani; matija.damjan@pf.uni-lj.si