

Številka: 0910-3/2026-28

Datum: 27. maj 2026

## Bo naslednjo škodo izplačala pametna pogodba?

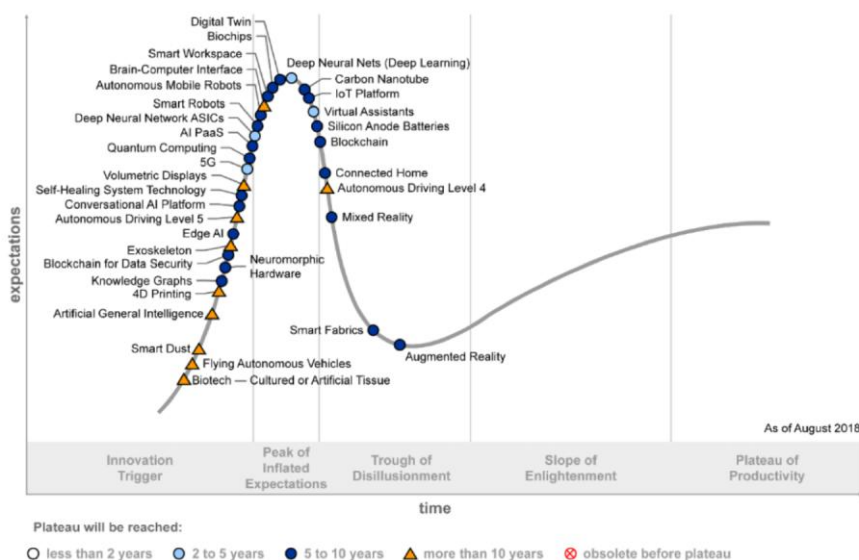
Tehnologija veriženja blokov je več kot le kriptovalute. V zavarovalništvu odpira možnosti za avtomatizirana plačila premij, hitrejša izplačila škod in uporabo pametnih pogodb. Ob tem pa se zastavljajo tudi vprašanja, ki zadevajo varnost, zaupanje in upoštevanje regulative.

Tehnologija veriženja blokov oziroma blockchain predstavlja enega izmed pomembnejših tehnoloških konceptov, ki spreminja način razumevanja in izvajanja nekaterih poslovnih procesov. Gre za tehnologijo, na kateri lahko temeljijo različne storitve, pametne pogodbe in koncepti Web3. Blockchain se zato ne nanaša zgolj na kriptovalute, temveč ga je mogoče uporabljati na različne načine.

Dne 13. 5. 2026 je bil na Združenju bank Slovenije izveden seminar z naslovom *Blockchain - od osnovnih konceptov, arhitektur in pametnih pogodb do web3*, katerega namen je bil udeležencem podati celovit, sodoben pregled zasnove in delovanja tehnologij veriženja blokov. Poseben poudarek je na arhitekturah, pametnih pogodbah, tokenizaciji sredstev, regulativi (MiCA, DLT pilot) ter konceptih Web3.

V okviru razvoja novih tehnologij je bil blockchain v preteklosti pogosto povezan s fazo velikega zanimanja oziroma t. i. hype fazo. Za ponazoritev razvoja pričakovanj glede novih tehnologij je uporabna Gartnerjeva krivulja *Emerging Technology Hype Cycle*, ki tehnologije razporeja glede na stopnjo pričakovanj, zrelosti in predviden čas do širše uporabe. Pri tem je treba upoštevati, da gre pri prikazu iz leta 2018 za takratno oceno stopnje zrelosti in pričakovanj glede posameznih tehnologij, ne pa nujno za aktualno stanje v letu 2026. Slika je zato uporabljena predvsem ilustrativno, kot prikaz tedanjega razumevanja razvoja tehnologije. Iz krivulje je razvidno, da so bile sprva močno izpostavljene kriptovalute, kasneje pa se je blockchain vse bolj začel obravnavati kot širši tehnološki koncept.

**Slika 1: Hype Cycle for Emerging Technologies, 2018**



*Vir: Gartner Identifies Five Emerging Technology Trends That Will Blur the Lines Between Human and Machine", 20. 8. 2018*

## Temeljni elementi tehnologije veriženja blokov

Blockchain temelji na treh osnovnih konceptih: **kriptografiji**, **podatkovnih bazah** in **porazdeljenem soglasju**. Ti elementi skupaj omogočajo, da se podatki oziroma transakcije varno zapisujejo, preverjajo in hranijo v omrežju, kjer ni nujno enega samega centralnega upravljavca.

### Kriptografija

Kriptografija je eden od osnovnih gradnikov blockchain tehnologije. Namenjena je zagotavljanju varnega prenosa podatkov in preverjanju, da podatki med prenosom niso bili spremenjeni. Pri blockchainu uporabniki med seboj izmenjujejo vrednost prek digitalnih denarnic. Če želi oseba A osebi B poslati na primer **kriptovaluto bitcoin (BTC)**, mora imeti programsko opremo oziroma digitalno denarnico. Digitalna denarnica pripravi transakcijo, v kateri je navedeno, kdo komu pošilja določeno vrednost. Takšna transakcija mora biti digitalno podpisana. Omrežje transakcije ne bo sprejelo, če ta ni digitalno podpisana s strani osebe, ki želi transakcijo izvesti.

Za razumevanje tega koncepta je pomembna razlika med simetrično in **asimetrično** kriptografijo, pri čemer se v Blockchainu uporablja asimetrična kriptografija. Pri simetrični kriptografiji se za šifriranje in dešifriranje uporablja isti ključ, zato je ključno vprašanje, kako ta ključ varno izmenjati. Pri asimetrični kriptografiji pa se uporabljata dva ključa: zasebni in javni ključ. Zasebni ključ ostane pri imetniku in je namenjen podpisovanju oziroma dokazovanju razpolagalne pravice, javni ključ pa omogoča preverjanje, ali podpis res ustreza določenemu zasebnemu ključu. Zasebni ključ je tisti, s katerim uporabnik nekaj podpiše oziroma dokaže, da je on tisti, ki želi izvesti določeno dejanje. Javni ključ pa omogoča preverjanje tega podpisa. Podoben koncept poznamo tudi pri kvalificiranih digitalnih potrdilih, na primer SIGEN-CA.

Pomemben del kriptografije so tudi **hash** oziroma zgoščevalne funkcije. Hash funkcija iz vhodnega podatka ustvari znakovni niz določene dolžine. Ne glede na to, ali je vhodni podatek kratek ali dolg, je rezultat vedno niz določene, vnaprej opredeljene dolžine znakov. Hash funkcije so deterministične v smislu, da isti vhodni podatek vedno da isti izhodni rezultat. Hkrati pa gre za enosmerne funkcije: iz rezultata ni mogoče enostavno ugotoviti, kakšen je bil prvotni vhodni podatek. V blockchainu se hash funkcije uporabljajo tudi za to, da se bloki med seboj povezujejo. Vsak blok vsebuje podatek o prejšnjem bloku, zato sprememba enega bloka vpliva na celotno verigo.

### Porazdeljene podatkovne baze

Blockchain je porazdeljena in decentralizirana podatkovna baza. Pri klasičnih sistemih ima običajno ena institucija (npr.: banka) nadzor nad podatki in infrastrukturo. Pri blockchainu pa ima več računalnikov oziroma vozlišč kopijo iste podatkovne baze. V primeru Bitcoina je osnovni zapis preprost: kdo komu pošlje koliko. Vsak računalnik v omrežju ima svojo kopijo podatkovne baze, zato govorimo o porazdeljeni podatkovni bazi. Namesto da bi en strežnik nadzoroval podatke, jih hrani več vozlišč. Pri decentralizirani bazi se pojavi vprašanje konsistentnosti. Če ni enega centralnega upravljavca, mora sistem na drug način zagotoviti, da vsi udeleženci sprejmejo isto različico podatkov. Zato je pri blockchainu ključen mehanizem porazdeljenega soglasja.

### Porazdeljeno soglasje: Proof of Work (PoW) in Proof of Stake (PoS)

Ena najbolj znanih oblik porazdeljenega soglasja je **Proof of Work** oziroma dokaz o delu, ki ga uporablja **Bitcoin**. Ta proces poznamo tudi kot rudarjenje. Pri tem rudarji tekmujejo v iskanju ustrezne rešitve kriptografskega problema. Poenostavljeno povedano: rudarji iščejo takšno vrednost, da bo hash bloka izpolnjeval določene pogoje, na primer da se začne z določenim številom ničel. Kdor prvi najde ustrezno rešitev, lahko predlaga nov blok transakcij in za to prejme nagrado. Blok praviloma vsebuje podatke o transakcijah, hash trenutnega bloka, hash prejšnjega bloka, časovni žig in dodatno vrednost, imenovano nonce. Ker vsak blok vsebuje referenco na prejšnji blok, so bloki povezani v verigo. Če bi nekdo želel spremeniti starejši blok, bi moral posledično spremeniti tudi vse naslednje bloke, kar je pri dovolj velikem in decentraliziranem omrežju izjemno težko.

Drugi pomemben model soglasja je **Proof of Stake** oziroma dokaz o deležu, ki ga uporablja npr.: **Ethereum (ETH)**. Pri tem se varnost omrežja ne zagotavlja z računsko močjo rudarjev, ampak z vložkom oziroma zaklenjenimi sredstvi validatorjev. Pri Proof of Stake se torej sredstva zaklenejo oziroma »stakajo«. Tisti, ki sodelujejo pri potrjevanju blokov, v sistem zaklenejo določeno količino kriptovalut, sistem pa nato po določenih pravilih izbira, kdo bo sodeloval pri potrjevanju novih blokov. Prednost tega modela je praviloma manjša energetska intenzivnost, odpira pa druga vprašanja, na primer koncentracijo vpliva pri večjih imetnikih sredstev.

### **Problem dvojne porabe**

Eden od osnovnih problemov digitalnega denarja je preprečevanje dvojne porabe oziroma *double spending*. V fizičnem svetu istega bankovca ni mogoče izročiti dvema osebam hkrati. V digitalnem svetu pa je podatke mogoče kopirati, zato mora sistem preprečiti, da bi ista digitalna vrednost bila porabljena dvakrat. Blockchain to rešuje tako, da se transakcije digitalno podpišejo in zapišejo v skupno evidenco. Vendar se pri decentraliziranem omrežju pojavi dodatno vprašanje: če pride do več transakcij, katera bo sprejeta kot veljavna? Ker v decentraliziranem omrežju ni enega centralnega časovnega sistema, se transakcije ne potrjujejo posamično vsako sekundo, ampak se združujejo v bloke. Zato je blockchain sestavljen iz blokov transakcij. Namesto da bi se omrežje usklajevalo za vsako posamezno transakcijo, se usklajuje glede skupka transakcij, ki so vključene v posamezen blok.

### **Pametna pogodba ni pogodba, ampak program**

Do pojava Etheruma se je govorilo predvsem o tehnologiji Blockchain 1.0, ki je bila povezana predvsem s prenosom digitalnih sredstev oziroma kriptosredstev. Z Ethereumom se pojavi **Blockchain 2.0**, ki poleg osnovnega prenosa vrednosti omogoča tudi **pametne pogodbe**.

Pametne pogodbe niso pogodbe v klasičnem pravnem smislu in niso nujno »pametne«. Gre predvsem za program, ki ga nekdo sprogramira in zapiše v blockchain omrežje. Pametna pogodba ima svoj naslov, stanje, kodo in lahko razpolaga s sredstvi. Ko je enkrat zapisana v blockchain omrežje, jo lahko uporabniki kličejo prek transakcij. Primer pametne pogodbe je program, v katerega več oseb pošlje določeno količino ETH. Program lahko določi pogoje, na primer minimalni vložek, maksimalno število udeležencev in način, kako se sredstva razdelijo. Ko so pogoji izpolnjeni, se koda izvede tako, kot je bila sprogramirana. Pametne pogodbe se lahko uporabljajo za različne primere, kot na primer za tokenizacijo, poravnavo transakcij, mikrotransakcije, avtomatizacijo procesov, avtomatizacijo plačil v dobi AI agentov in napovedne trge.

### **Možna uporaba tudi v zavarovalništvu**

Uporaba pametnih pogodb bi lahko prišla v poštev tudi v svetu zavarovalništva. Zavarovalnica bi lahko tako pripravila pametno pogodbo, ki omogoča avtomatizirano plačilo premije in izplačilo v primeru določenega dogodka. Uporabnik bi s svojo denarnico poklical pametno pogodbo, poslal znesek in morebitne potrebne podatke oziroma dokazila, pri čemer bi bilo treba posebej paziti na varstvo osebnih podatkov. Pametna pogodba bi preverila, ali je bilo plačilo pravilno. Če do določenega dogodka ne bi prišlo, bi se sredstva lahko prenesla zavarovalnici. Če bi do dogodka prišlo, bi uporabnik lahko zahteval izplačilo.

Pri samem procesu izplačila stranki zaradi škodnega dogodka se pojavi vprašanje, kako pametna pogodba ve, ali se je dogodek res zgodil. Ker pametna pogodba sama ne more preverjati podatkov iz zunanjega sveta ne more sama ugotoviti, ali je bila toča, ali je bil let odpovedan, ali je prišlo do zamude. Zato potrebuje zunanji vir podatkov, ki se imenuje **orakelj**. Orakelj je storitev, ki pametni pogodbi posreduje zunanji podatek. Pametna pogodba nato na podlagi tega podatka izvede določeno dejanje. Pri tem je bistveno, da gre za vir podatkov, ki mu sistem zaupa.

Takšna uporaba je posebej primerna pri enostavnejših in objektivno preverljivih dogodkih, na primer zamudi leta, odpovedi leta ali določenem vremenskem dogodku, medtem ko so kompleksnejše škode, ki zahtevajo presojo, za popolno avtomatizacijo zahtevnejše.

Pametne pogodbe imajo tudi pomembne omejitve. Ena od ključnih težav je, da se pametne pogodbe po tem, ko so zapisane v blockchain omrežje, praviloma ne morejo enostavno spreminjati. Če je v kodi napaka, je zato ni mogoče preprosto popraviti. To pomeni, da je pri pametnih pogodbah zelo pomembno, kako so zasnovane in sprogramirane.

### **Blockchain kot sistem zaupanja brez centralnega posrednika**

Blockchain je tehnologija, ki temelji na kriptografiji, porazdeljenih podatkovnih bazah in porazdeljenem soglasju. Njegov osnovni namen je omogočiti zanesljiv zapis in prenos podatkov oziroma vrednosti v okolju, kjer ni nujno enega samega centralnega posrednika.

Razvoj od Blockchain 1.0 do Blockchain 2.0 je omogočil prehod od osnovnega prenosa kriptovalut k pametnim pogodbam, tokenizaciji in širšim Web3 konceptom. Pri tem pa ostajajo pomembna vprašanja arhitekture, varnosti, upravljanja ključev, zanesljivosti orakljev, stroškov izvajanja, možnosti napak v pametnih pogodbah ter regulativne skladnosti.

Če poenostavimo, blockchain ni ena sama tehnologija ali ena sama aplikacija, temveč kombinacija več tehnoloških pristopov, ki skupaj omogočajo zanesljiv in preverljiv zapis podatkov med več udeleženci.

Agencija za zavarovalni nadzor

#### **KONTAKTI:**

telefon: + 386 (1) 2528 600

telefaks: + 386 (1) 2528 630

e-mail: [agencija@a-zn.si](mailto:agencija@a-zn.si)

www: <http://www.a-zn.si/>

Twitter: [@AZN\\_PR](https://twitter.com/AZN_PR)

---

### **O Agenciji za zavarovalni nadzor**

Agencija je bila ustanovljena junija 2000 na podlagi Zakona o zavarovalništvu. Cilj državne nadzorne institucije na področju zavarovalništva je zmanjševanje in odpravljanje nepravilnosti v zavarovanju, varovanje interesov zavarovalcev in omogočanje delovanja zavarovalnega gospodarstva ter pozitivnega vplivanja le-tega na celotno gospodarstvo. Agencija je pri svojem delu neodvisna in samostojna.



**Družbeno  
odgovoren  
delodajalec**

Napredni certifikat H.3. 0014/2020 - NI



**EVROPSKA UNIJA**  
EVROPSKI  
SOCIALNI SKLAD

NALOŽBA V VAŠO PRIHODNOST

Naložbo sofinancirata Republika Slovenija in Evropska unija iz Evropskega socialnega