KOFETKE.

Mreže agentov, Web3 in denarni tokovi

Katere nove povezave so koristne in katere povečujejo tveganje, ne da bi rešile težavo?



MREŽE IN PLAČILA

Stvaren pregled orodij, predaj nalog med agenti, plačilnih protokolov in meja pooblastil.

SLOVENSKA IZDAJA

september 2026
Praktična uporaba AI

Viri preverjeni 21. septembra 2026.

Besedna zveza »mreža agentov« lahko ustvari vtis, da se običajna programska ureditev organizira sama in je donosna. Navadno pomeni, da si več programov med seboj predaja naloge, podatke ali zahteve. To je lahko koristno. Preden ustvari en sam zanesljiv rezultat, pa lahko tudi pomnoži stroške, dovoljenja in poti do napak.

Praktično vprašanje ni, ali se bodo programski agenti med seboj pogovarjali. To že lahko počnejo. Vprašanje je, kaj sme posamezen sistem početi, kako se njegovo delo preverja in ali bo stranka plačala za rezultat, ki je vreden plačila tudi ob upoštevanju stroškov računalniške obdelave, človeškega pregleda, podpore in napak. Protokol lahko olajša povezovanje ali plačevanje. Ne more ustvariti povpraševanja, jamčiti kakovosti izhoda ali iz nenadzorovanih procesov narediti podjetja.

Ta članek loči štiri plasti, ki se pogosto mešajo: povezovanje modela z orodji in kontekstom; predajanje naloge drugemu agentu; dokazovanje identitete in pooblastil; ter premikanje denarja. Če jih obdržite ločene, je zasnovo veliko lažje pregledovati.

Štiri plasti, štiri različne obljube

Plast	Praktična naloga	Ne dokazuje
Kontekst in orodja	Aplikaciji omogočijo branje vira ali klic določene funkcije	da je orodje varno, da je vhod zaupanja vreden ali da je dejanje odobreno
Predajanje nalog med agenti	Pošljejo nalogo drugi storitvi ter prejmejo napredek ali artefakt	da je storitev sposobna, plačilno sposobna, poštena ali da sme porabljati denar
Identiteta in pooblastila	Prepoznajo klicatelja in omejijo, do česa lahko dostopa ali kaj lahko naredi	da je zahtevano dejanje smiselno ali dobičkonosno
Plačilo	Zahtevajo, odobrijo, preverijo in poravnajo bremenitev	da ima kupljeni izhod vrednost, da je pravilno prispel ali da ga je mogoče povrniti

Model Context Protocol (MCP) sodi predvsem v prvo vrstico. Standardizira povezavo med aplikacijo AI in strežniki, ki ponujajo vire, pozive in orodja. Trenutna specifikacija orodja opisuje kot funkcije, ki jih lahko izvede model, vire pa kot kontekst in podatke.[43] Strežnik MCP bi lahko izpostavil katalog izdelkov samo za branje, iskalno funkcijo po omejenem naboru

dokumentov ali funkcijo, ki ustvari zapis osnutka. Iz modela ne naredi zaupanja vrednega zaposlenega. Ne pozna poslovnih pravil podjetja, razen če jih uveljavlja gostiteljska aplikacija.

Zato je lokalna konfiguracija vredna pozornosti. Opis orodja je le opis. Specifikacija MCP pravi, da morajo uporabniki izrecno privoliti v dostop do podatkov in postopke, opise vedenja orodij pa obravnava kot nezaupanja vredne, razen kadar izvirajo z zaupanja vrednega strežnika.[43] Orodni strežnik tretje osebe ima lahko uglajeno ime, vendar kljub temu zahteva podatke ali dejanja, ki presegajo njegov zatrjevani namen. Začnite z majhnim seznamom dovoljenih možnosti, vidnimi vhodi in izhodi, kratkotrajnimi poverilnicami ter jasno potrditvijo pred zunanjimi učinki, kot so pošiljanje, naročanje, brisanje ali objavljanje.

Agent2Agent (A2A) sodi predvsem v drugo vrstico. Neodvisnim agentom omogoča odkrivanje zmogljivosti, izmenjavo sporočil, upravljanje nalog s stanjem in vračanje artefaktov. A2A nalogo opredeljuje kot temeljno enoto dela z ID-jem in življenjskim ciklom.[44] Klicatelj lahko preveri stanje naloge in zahteva preklic, vendar specifikacija pravi, da uspeh preklica ni zagotovljen.[44] Delo je morda že končano ali je doseglo stopnjo, ki je ni mogoče preklicati. Zahteva za preklic zato ni dokaz, da ni prišlo do nobenega sporočila, spremembe zapisa ali plačila; aplikacija še vedno potrebuje zaščito pred podvajanjem, končno preverjanje pooblastila pred zunanjim dejanjem in pot za obnovitev.

MCP in A2A je mogoče uporabljati skupaj. Raziskovalni agent lahko prejme nalogo A2A za primerjavo treh dokumentov; znotraj svoje meje lahko uporabi orodja MCP za iskanje po dovoljenem indeksu virov in shranjevanje artefakta. Specifikacija A2A to

delitev izrecno opisuje: MCP povezuje modele ali agente z orodji, API-ji in podatki, A2A pa je namenjen sodelovanju in predajanju dela med neodvisnimi agenti.[44] Noben protokol ne odloča, ali raziskovalni agent sme brati zasebne datoteke, govoriti z dobaviteljem, odobriti račun ali rezultat deliti navzven. To so odločitve o pooblastilih zunaj transportnega sloja.

Identiteta in pooblastila potrebujejo ločeno zasnovo. OAuth 2.0 ponuja uporaben splošni vzorec: loči odjemalca od lastnika vira in izda dostopni žeton z obsegom in rokom veljavnosti, namesto da bi predal glavne poverilnice lastnika.[46] Natančna tehnologija je lahko drugačna, vendar načelo ostaja. Agent, ki sme brati cenik, nima samodejno dovoljenja, da ga spreminja. Agent, ki lahko pripravi osnutek sporočila, nima dovoljenja, da ga pošlje. Agent, ki lahko zahteva plačljivo storitev, ne bi smel imeti splošnega ključa denarnice ali stalne možnosti kupiti kar koli najde.

Omejena farma AI

»Farma AI« je skupina delavcev, navadno klicev modelov skupaj s kodo, ki obdelujejo naloge iz čakalne vrste. V smiselni manjši uvedbi je omejena: ima znane vrste nalog, končno sočasnost, omejitve porabe, časovne omejitve, shranjene artefakte in lastnika, ki jo lahko ustavi. Beseda farma naj ne bi nakazovala organizma, ki služi, medtem ko njegov lastnik spi.

```
Odobren sprejem nalog
    |
preverjanje sheme
    +-> zavrni / zahtevaj manjkajoča polja
    |
čakalna vrsta s prednostjo, proračunom in rokom
    |
skupina izvajalnih procesov
(določena sočasnost, brez skritih poverilnic)
    |
artefakt + viri + dnevnik izvajanja + zapis stroška
    |
deterministična preverjanja / človeški pregled
    |
odobrena dostava ali zavrženje
```

Koristna enota je pogodba o nalogi. Določa vhodno shemo, dovoljene vire ali orodja, največje število klicev modela, rok, pričakovani artefakt, sprejemni preizkus, lastnika in pot za eskalacijo. Delavec lahko nato nadzorovano zaključi z napako: »v dovoljenem indeksu ni bil najden noben vir« je bolje kot izmišljen odgovor; »omejitev proračuna je bila dosežena pred dokončanjem izvlečka« je bolje kot odprta zanka ponovnih poskusov.

Izmišljen primer. Majhna prevajalska agencija vsak teden prejme petdeset posodobitev opisov izdelkov. Želi omejen sistem, ki pripravi paket za pregled, ne pa da samodejno objavlja prevode. Vsaka naloga vsebuje ID izdelka, različico izvornega besedila in ciljne jezikovne in področne nastavitve. Razčlenjevalnik zavrne manjkajoče ID-je. Hkrati lahko delujeta dva izvajalna procesa. Vsak lahko bere le priloženi zapis izdelka in terminološki seznam, lahko opravi največ tri klice modela ter zapiše predlagani prevod,

seznam spremenjenih izrazov, različico vira in opombe o ocenjeni zanesljivosti. Deterministično preverjanje potrdi, da sta ID izdelka in zahtevani varnostni stavek še vedno prisotna. Jezikovni strokovnjak paket sprejme, uredi ali zavrne. Če terminološka storitev ni na voljo, se naloga ustavi in sporoči odvisnost, namesto da bi uporabila spletno iskanje kot nadomestek.

Tak sistem lahko zmanjša količino ponavljajoče se priprave. Še vedno pa ima stroške: uporabo modela, programsko opremo za čakalno vrsto, čas pregleda, spremljanje, spremembe pri ponudnikih in odpravljanje občasnega slabega rezultata. Njegovo merilo uspeha ni število nalog. To je sprejet paket za pregled, ki prihrani dovolj preverjenega dela ali prepreči dovolj napak, da upraviči skupni strošek.

Farma potrebuje tudi zanesljivostne nadzore, ki zvenijo manj glamurozno kot »večagentni sistem«. Idempotentnost prepreči, da bi ponovni poskus ustvaril dva zapisa ali dve bremenitvi. Čakalna vrsta mrtvih sporočil zadrži naloge, ki večkrat ne uspejo, namesto da bi se vrtele v nedogled. Omejitve hitrosti ščitijo zunanje storitve. Različice navodil modelu, identifikatorji modelov in sheme orodij pomagajo rekonstruirati pogoje, ki so privedli do nepričakovanega izhoda. Ne zagotavljajo enakega rezultata nedeterminističnega modela. Sled naj poveže ID naloge z vhodno različico, URL-ji virov, klici orodij, zgoščeno vrednostjo artefakta, odločitvijo pregledovalca in stroškom. Okvir NIST umešča upravljanje skozi celoten proces obvladovanja tveganj, kar je koristen opomnik, da sta beleženje in pregled značilnosti sistema, ne pa končni dokument o skladnosti.**[42]**

Plačilo je omejena zmožnost

x402 podpira izmenjavo, pri kateri je potrebno plačilo, med programskimi sistemi. V različici 2 so njegove temeljne zahteve glede plačila, strukture koristnega tovora in poravnave neodvisne od transporta; HTTP, MCP in A2A so med transporti, prek katerih so lahko predstavljene.[45] Integracije HTTP uporabljajo vzorec HTTP 402 payment-required, vendar to ni opredelitev vsake integracije x402.[45] V preprostem toku strežnik vira sporoči, da je potrebno plačilo, odjemalec predloži podpisano odobritev, posrednik pa preveri in poravna v skladu s plačilno shemo in omrežjem.[45]

To je lahko koristno za API-klic z določeno ceno ali zaščiten digitalni vir, kadar uporabniški račun ni potreben ali je nepraktičen. To je plačilni mehanizem. Ne vzpostavlja identitete v širšem poslovnem smislu, ne ocenjuje dobavitelja, ne dokazuje pravilnosti rezultata API-ja, ne upravlja davčnih obveznosti, ne obravnava vračil, ne rešuje potrošniškega spora in ne naredi nakupa gospodarsko upravičenega. Citirana specifikacija sama postavlja za transport specifične izvedbe zunaj svojega temeljnega obsega.[45] Prav v teh podrobnostih se skriva veliko operativnih težav.

Plačilni tok mora biti tesneje omejen kot orodje za pridobivanje informacij. Odobritev naj navede določeno storitev, vir ali naročilo, najvišji znesek, rok veljavnosti, dovoljeno sredstvo ali valuto ter enolično referenco. Ločena storitev naj preveri rezultat. Sistem mora zabeležiti, ali je bilo delo dostavljeno, ne le ali je zahteva za plačilo vrnila uspeh. Če lahko ena naloga povzroči

vrsto bremenitev, ji določite skupno zgornjo mejo in pogoj ustavitve; sicer zanka, ki še naprej išče »še en vir«, postane incident pri zaračunavanju.

Kripto je lahko eden od neobveznih načinov za poravnavo stroškov med stroji. Ni zahteva za agente, MCP, A2A, klicanje orodij ali čakalno vrsto nalog. Običajno izdajanje računov, naročniški računi, vnaprej plačani dobropisi, naročilnice in kartično procesiranje lahko mnogim organizacijam bolj ustrezajo. Izbira je odvisna od nasprotnih strank, računovodstva, varstva potrošnikov, lokalnih pravnih obveznosti, tveganja skrbništva in pogostosti nakupa storitve. Gre za izbiro infrastrukture, ne za priporočilo sredstva.

Skrbništvo nad ključi je težaven rob te izbire. Zasebni ključ ali široko pooblastilo za podpisovanje ni neškodljiva konfiguracijska vrednost. Če ga daste agentu, postanejo njegovo navodilo modelu, veriga orodij, dnevniki in izvajalno okolje del varnostne meje. Uporabite najmanjša možna pooblastila: ločen račun ali storitev, stroge omejitve na transakcijo in na dan, dovoljene cilje, kratke roke veljavnosti, potrditev za neznane prejemnike in hitro pot za preklic. Skrivnih ključev nikoli ne vnašajte v navodila modelu, dokumente, profile brskalnika ali običajne dnevnike. Storitev, ki za delovanje potrebuje ključ, mora biti zasnovana ob predpostavki možnosti kompromitacije, ne na zaupanju v namere modela. Smernice OWASP opozarjajo, da generativna AI širi tako zmožnosti agentov kot povezana tveganja.**[47]**

Kaj Web3 spremeni in česa pusti pri miru

Web3 tukaj pomeni ureditve, ki kot del aplikacije uporabljajo denarnice, zapise v verigi blokov ali storitve, zasnovane na žetonih. Ni pogoj, da model bere dokument, pokliče orodje ali preda delo drugemu agentu. Pri zasnovi plačevanja za posamezne zahteve, kot je x402, je zanimiva možnost, da program kupi en določen vir, kadar ga potrebuje, v okviru vnaprej določene politike, namesto da bi oseba urejala še eno ponavljajočo se naročnino.[45] Ali je to priročno, je odvisno od storitve in ljudi, ki jo uporabljajo.

Plačilni zapis in zapis o delu še vedno odgovarjata na različni vprašanji. Poravnana bremenitev ne dokazuje, da je dokument prispel, da je njegova vsebina točna ali da je imel kupec dovoljenje za deljenje vhoda. Aplikacija potrebuje ločene zapise za te izide. Uvedba denarnice spremeni zasnovo plačevanja in skrbništva; ne odstrani preostanka dela.

Od mehanizma do posla

Vzdržna storitev potrebuje plačljive stranke in ceno, ki pokrije njene dejanske stroške. Pripravljenost plačati ni dokaz ponovljivega povpraševanja, prihodek pa ni dobiček. Plačilne poti ne rešijo težjih delov:

Poslovno vprašanje	Potrebni operativni dokazi
Kdo ima težavo?	določena stranka in ponavljajoče se delo, ne splošno občinstvo

Poslovno vprašanje	Potrebni operativni dokazi
Kaj je dostavljeno?	artefakt, ki ga je mogoče pregledati, raven storitve ali dokončana transakcija
Zakaj mu zaupati?	preverjanja kakovosti, izvor, pot za popravke in odgovoren upravljavec
Koliko stane izvedba?	stroški modela, podatkov, računanja, človeškega pregleda, podpore, plačil in napak
Ali se lahko ponovi?	stabilni vhodi, dovoljenje za njihovo uporabo, varen delovni tok in povpraševanje, ki presega enkraten nakup iz novosti

Ilustrativna serija konkretizira vprašanje stroška. Predpostavimo, da klici modela stanejo 5 €, pregled traja pol ure in je ovrednoten na 30 € na uro, sprejetih pa je dvajset izhodov. Neposredni strošek modela in pregleda je **€5 + (0.5 × €30) = €20**, oziroma **€20 ÷ 20 = €1** na sprejeti izhod. To so izmišljeni vnosi za izračun, ne cene dobaviteljev ali sporočen prihranek. Dodati bi bilo treba še stroške infrastrukture, licenc za podatke, podpore in plačil. Zavrnjeno delo sodi v števec, čeprav ne ustvari ničesar, kar bi bilo mogoče prodati; če bi delili le s številom vseh poskušenih nalog, bi uporaben izhod prikazali kot cenejšega, kot je v resnici.

Razmislite o dveh izmišljenih ponudbah. Prva je »avtonomni agent za tržne raziskave, ki najde priložnosti za dobiček«. Nima določenega kupca, nobenega preizkusa za dobro priložnost,

pravice do podatkov so nejasne, odgovornost ni opredeljena in finančna obljuba nima podlage. Dodatek gumba za plačilo z žetoni ne spremeni ničesar od tega.

Druga je storitev, ki za tri gradbene podizvajalce pripravi dokumentiran tedenski povzetek uradnih obvestil o javnem naročanju v eni regiji. Njeni vhodni viri so navedeni; izhod je datirana preglednica s povezavami in možnostjo ročnega pregleda; izključuje pravno svetovanje in oddajo ponudb. Primerna bi lahko bila naročnina ali račun. Končna točka x402 bi bila tehnično mogoča za en sam plačljivi izvoz, vendar ni nujno najboljša izkušnja za stranko. Poslovni primer je odvisen od tega, ali so povzetki točni, pravočasni in vredni stroškov ponudnika.

Protokoli so koristni, kadar odstranijo oviro pri integraciji. Čakalna vrsta je koristna, kadar naredi omejeno delo opazno. Zahteva za plačilo je koristna, kadar zaračuna za znan vir pod znanim pooblastilom. Nič od tega ne nadomesti jasne ponudbe, odgovornega upravljavca ali stranke, ki ima korist. Trezen cilj zasnove je sistem, ki lahko pove, kaj je naredil, koliko je stal, kaj je smel narediti in kdaj se je ustavil.

Viri

Številke virov sledijo skupnemu seznamu. Povezave vodijo do izvirnih dokumentov. Pogoji uporabe in razpoložljivost storitev se lahko spremenijo.

[42] NIST AI Risk Management Framework 1.0
https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf

[43] Model Context Protocol Specification
https://modelcontextprotocol.io/specification/2025-11-25

[44] A2A Protocol Specification
https://a2a-protocol.org/latest/specification

[45] x402 Protocol Specification v2
https://raw.githubusercontent.com/coinbase/x402/main/specs/x402-specification-v2.md

[46] RFC 6749: OAuth 2.0 Authorization Framework
https://www.rfc-editor.org/rfc/rfc6749.html

[47] OWASP Agentic AI: Threats and Mitigations
https://genai.owasp.org/resource/agentic-ai-threats-and-mitigations