

10 ottobre 2023 15:43

CLIAPI 9 - Microsoft Autogen: i multi-agenti autonomi cambieranno l'AI

di [Alessandro Pedone](#)

In questo nono articolo della serie

“Capire L’Intelligenza Artificiale Per Investirci” desidero proporre una evoluzione di quei software che, impropriamente, ci siamo abituati a chiamare “Intelligenze Artificiali Generative”. [Il primo articolo](#), scritto ad inizio anno, è partito proprio con Chat GPT, il motore LLM (Large Language Model, modelli di linguaggio di grandi dimensioni) più utilizzato al mondo, prodotto da OpenAI, azienda che ha una partnership molto rilevante con Microsoft di cui parleremo molto in questo articolo. Per scrivere quanto segue, abbiamo tratto molta ispirazione dai contenuti della conferenza Future Technologies Conference 2021 tenuta dal prof. **Michael Wooldridge** della Oxford University e direttore per l’intelligenza artificiale del prestigioso Alan Turing Institute sul tema degli agenti autonomi.

La delega, l’umanizzazione e “intelligenza”

L’avvento degli smartphone (o simili) che sono con noi 24 ore al giorno, collegati costantemente alla rete, è una realtà che ha circa quindici anni ed ha letteralmente cambiato il mondo. Abbiamo processori informativi - sempre più potenti - ovunque, interconnessi, che possono comunicare tra loro. L’incremento della potenza di calcolo, l’ubiquità e l’interconnessione sono le tre tendenze più importanti dell’informatica negli scorsi decenni.

Le prossime tre tendenze più importanti che si realizzeranno su vastissima scala nei prossimi decenni saranno: la delega, l’“umanizzazione” e l’“intelligenza”.

Deleghiamo sempre più compiti ai computer, consegniamo sempre più controllo delle nostre vite, facciamo fare sempre più cose per nostro conto.

Negli anni '80, il grande dibattito dell'epoca riguardava gli aerei fly-by-wire, l'idea di avere aerei con sistemi di controllo computerizzati in cui gli esseri umani non erano all'interno del sistema, non controllavano direttamente l'aereo. Anche se oggi nessuno si sognerebbe di metterli in discussione, quei sistemi all'epoca erano molto controversi così come oggi - ed ancora più nei prossimi anni - lo sono le auto senza conducente. Sarà sempre più normale affidare a degli agenti la realizzazione di compiti importanti che oggi richiedono l'azione degli esseri umani.

Nel mondo della finanza, il fenomeno dell'High Frequency Trading è un esempio (non solo positivo, per usare un eufemismo) di quanto abbiamo delegato alle macchine questioni economicamente estremamente rilevanti. Una parte molto consistente della negoziazione dei titoli che avvengono quotidianamente non è decisa da esseri umani, ma da macchine che eseguono negoziazioni di acquisto e vendita alla velocità di frazioni di secondo, cosa che sarebbe impossibile per un essere umano.

Per tendenza verso "l'umanizzazione" intendo il fatto che interagiamo con questi agenti in modo sempre più simile a come faremmo con un essere umano. L'esempio degli assistenti digitali domestici come Alexa o Google Assistant sono un esempio, sebbene non siano ancora così brillanti nell'interagire con il linguaggio umano, specialmente se confrontati agli agenti come Chat GPT o Google Bard.

L'ultima tendenza rilevante è ciò che chiamiamo, impropriamente, intelligenza. In realtà dovremmo proprio chiamarla "agentività", ma il termine non è giornalmisticamente efficace e quindi dobbiamo rassegnarci ad usare questo termine estremamente fuorviante. Con "intelligenza" intendiamo la tendenza a sviluppare macchine sempre più capaci di compiere azioni che richiederebbero intelligenza se fossero compiute da esseri umani. Negli ultimi anni questa tendenza è aumentata notevolmente e quest'anno è esplosa con lo sviluppo dei modelli di linguaggio di grandi dimensioni (LLM).

Ad oggi, quindi, stiamo costruendo sempre di più degli **agenti** informatici seguendo queste sei tendenze:

1. sempre maggiore **potenza di calcolo**;
2. diffusa praticamente **ovunque**;
3. sempre **interconnessa**;
4. alla quale **deleghiamo** compiti fondamentali per gli esseri umani;
5. con la quale interagiamo **come** faremmo con **esseri umani**;
6. dotata di una capacità di agire che se fosse svolta da esseri umani richiederebbe sempre più **intelligenza**.

Se tutto questo è vero, com'è vero, quale sarà mai il passo conseguente?

Multi-agenti autonomi che interagiscono fra loro

Il prof. Michael Wooldridge ha dedicato buona parte della sua carriera accademica a studiare come dotare questi agenti di **abilità sociali**, per farli interagire fra di loro, sviluppando la capacità di cooperare, coordinarsi e negoziare con altri agenti.

queste sono abilità sociali e storicamente, una delle cose un po' strane dell'intelligenza artificiale è che per circa metà della sua storia, l'IA non ha pensato a questo tipo di abilità. Le cose di cui l'IA si preoccupava erano principalmente cose come la risoluzione di problemi e la pianificazione, che sono in gran parte cose che un sistema di intelligenza artificiale fa da solo, e le questioni su cosa accada quando i sistemi di intelligenza artificiale parlano tra di loro sono state in gran parte ignorate dalla comunità. Ma la mia ricerca si è concentrata esclusivamente sulla costruzione di sistemi di IA con queste abilità, la capacità di cooperare, coordinarsi e negoziare. Questo significa essere in grado di sapere quando è il momento giusto per condividere informazioni. Sapere che non bisogna bombardare gli altri agenti con informazioni, ma farlo esattamente al momento opportuno.

L'idea alla base è quella di avere una 'squadra' di agenti che dialogano fra loro, proprio come nelle squadre umane: ci sono esseri umani specializzati in diversi compiti (più operativi, di coordinamento, di controllo, decisionali, ecc.). In modo simile, ci saranno agenti specializzati nello scrivere codice, altri nel fare delle verifiche, altri nell'eseguire tale codice e riportare eventuali errori, altri ancora nel dialogare con gli esseri umani per ricevere le istruzioni e comunicare i risultati, e altri ancora - molto importanti - che coordinano il lavoro di questi robot. Il lavoro che svolge il prof. Michael Wooldridge con il suo team è costruire protocolli e tecniche che questi agenti possono utilizzare per cooperare fra di loro. Wooldridge lavora prevalentemente con robot, ma gli stessi concetti sono utilmente applicati anche per gli agenti software. Il fatto che il compito sia eseguito non più soltanto da un unico agente, ma da una pluralità di agenti aventi caratteristiche diverse aumenta in modo esponenziale sia la complessità che le potenzialità del sistema. Si aprono tutta una serie di nuove possibilità che fino ad oggi non sembravano alla portata dei software così come li conosciamo oggi. Tutto questo può apparire un po' fantascienza ma - come vedremo nel prossimo paragrafo - non è affatto così.

Microsoft AutoGen

Nel corso di questo 2023 sono stati presentati diversi ambienti di programmazione che consentono di creare sistemi di intelligenza artificiale generativa multi-agenti, alcuni dei quali sono anche open-source.

Il 25 settembre scorso Microsoft Research ha [presentato AutoGen](#), una libreria open-source per la realizzazione dei nuovi software basati sui modelli di linguaggio di grandi dimensioni (LLM) in grado di fare cose apparentemente

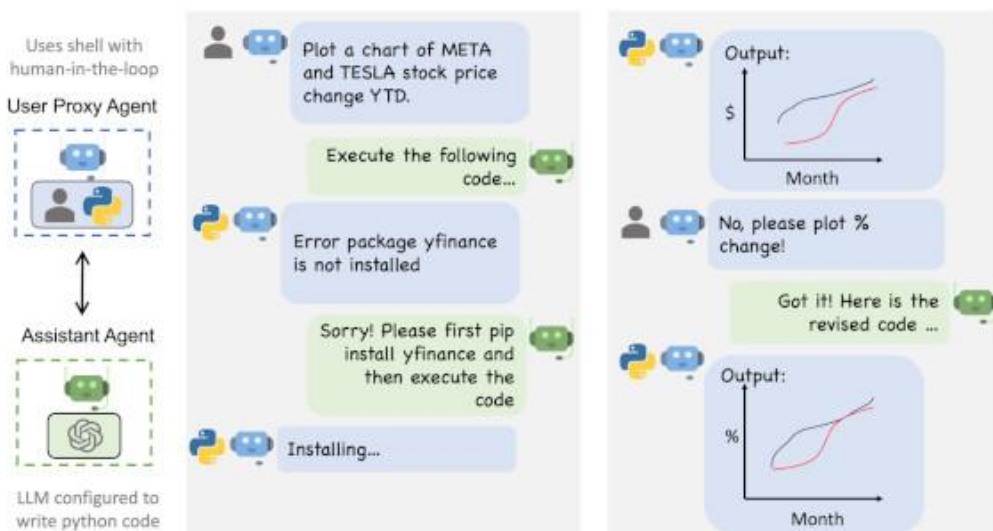
“magiche”. Il fatto che l'ambiente sia di Microsoft fornisce a questo strumento una potenzialità di diffusione incredibilmente maggiore rispetto ai modelli visti fino ad oggi.

La prima volta che ho visto la presentazione di questo framework sono rimasto letteralmente senza parole.

AutoGen è pensato per gli sviluppatori di software. Chi non ha un po' di dimestichezza con i linguaggi di programma (in particolare Python) può avere l'impressione che sia una cosa complicatissima.

In realtà è vero esattamente l'opposto. Il framework si occupa di tutti gli aspetti veramente complicati legati alla comunicazione fra i vari agenti. Tutto quello che deve fare lo sviluppatore è definire i vari agenti che collaborano fra di loro e farlo è veramente semplicissimo, alla portata di chiunque abbia i rudimenti di programmazione in Python. La magia consiste nel fatto che una volta definiti i vari agenti, questi inizieranno a parlare fra di loro fino a restituire il risultato finale all'utente.

Nello schema della figura seguente si vedono definiti solo due agenti. Il primo, definito come “User Proxy” riceve il comando dall'umano e interagisce con l'altro agente definito “Assistant” che ha l'abilità di scrivere il codice che verrà eseguito da User Proxy, valutato ed - eventualmente - utilizzato per fornire la risposta all'umano.



Nello schema si vede che l'umano chiede all' User Proxy di disegnare un grafico con le variazioni da inizio anno dei prezzi delle azioni di Tesla e di Meta. User Proxy gira la richiesta ad Assistant il quale restituisce il codice Python per eseguire la richiesta. User Proxy prova ad eseguire il codice, ma il codice non funziona ed allora comunica ad Assistant il tipo di errore che riceve, Assistant modifica il codice per farlo funzionare ed effettivamente funziona, ma User Proxy si accorge che il grafico non mostra le variazioni, ma direttamente i prezzi, quindi chiede ancora ad Assistant di modificare il codice per disegnare il grafico con le percentuali, non con i prezzi. Assistant finalmente restituisce il codice corretto e User Proxy mostra il grafico all'umano.

Questo è un esempio molto semplice con due soli agenti, ma lo stesso concetto si può applicare a casi molto più complessi.

Le potenzialità di uno strumento del genere sono inimmaginabili. Come ho più volte scritto in questa serie di articoli, quella che chiamiamo intelligenza artificiale è prima di ogni altra cosa una rivoluzione copernicana nel modo in cui scriviamo il software. Da software prevalentemente deterministici a software prevalentemente probabilistici.

Microsoft e l'intelligenza artificiale

Microsoft e Google sono due fra le grandissime aziende della tecnologia che maggiormente vedranno il loro business trasformato dall'intelligenza artificiale. Al momento Microsoft si sta muovendo con maggiore tempismo e spregiudicatezza rispetto a Google. La collaborazione fra OpenAI e Microsoft, per quanto sia vitale per OpenAI, porterà molti più vantaggi a Microsoft di quanto ne porterà ad OpenAI.

AutoGen è uno strumento il cui potenziale lascia attoniti eppure è solo uno dei numerosi progetti di Microsoft nel mondo dell'intelligenza artificiale.

Microsoft ha ben appreso la dura lezione che ha imparato ai tempi della rivoluzione di Internet, quando comprese tardi l'importanza della rete e ci si buttò tentando di essere lo standard.

Questa volta sta saltando a cavallo della rivoluzione dell'intelligenza artificiale diventando protagonista senza

velleità egemoni e collaborando - senza legarsi le mani - con le realtà più innovative.

Tutta l'offerta software di Microsoft si sta permeando delle migliori funzionalità oggi possibili grazie all'intelligenza artificiale e sostanzialmente non sta perdendo un colpo.

Personalmente non credo che Microsoft diventi la più importante azienda nel mondo dell'intelligenza artificiale nel giro di 5-10 anni. Microsoft è un colosso, come Google, e questi colossi inevitabilmente non hanno l'agilità necessaria. L'attuale gestione è sicuramente illuminata e sta facendo il massimo per essere una protagonista importante, ma non credo che sarà la principale. Come ho già scritto nei precedenti articoli, credo che il fatturato maggiore in questo settore toccherà a Tesla, grazie alla guida autonoma. La seconda azienda che potrebbe diventare la più importante - a mio giudizio - è Palantir, poiché l'infrastruttura software che ha costruito in diversi anni è perfetta per sposarsi con i vari modelli di intelligenza artificiale. La penetrazione che ha già conquistato nel settore governativo (e quella che sta conquistando nel settore delle grandi aziende), unita all'agilità di un'azienda grande, ma non enorme, la mette nelle migliori condizioni per diventare la leader nel nuovo mondo dell'informatica che sta nascendo. Si tratta, infatti, di un mondo che non ruota più attorno al vecchio software deterministico (che usava i dati), bensì è l'inverso, ruota attorno ai dati che usano i vari modelli di intelligenza artificiale.

Questo richiede una infrastruttura che né Microsoft, né Google né altri colossi del vecchio mondo dell'informatica hanno.

Dopo Tesla e Palantir, però, ritengo che Microsoft, Google e Nvidia, fra i vecchi colossi, possano essere le aziende che maggiormente si avvantaggeranno di questa rivoluzione in atto. Fra queste tre, Microsoft è quella che preferisco per svariate ragioni, ma prevalentemente perché ha il management decisamente migliore.

CHI PAGA ADUC

l'associazione non **percepisce ed è contraria ai finanziamenti pubblici** (anche il 5 per mille)

La sua forza economica sono iscrizioni e contributi donati da chi la ritiene utile

DONA ORA (<http://www.aduc.it/info/sostienici.php>)