Vibin Labs

The Fintagonist

Is The AI Machine A Worker Or The Boss? Answer This Carefully When Building Agentic AI Apps

If it's Saturday (or Tuesday), it must be the Fintagonist. Fin, Pro, An, The Fintagonist, a contrarian's view on software manufacturing with artificial intelligence in the financial services and fintech space. Bringing unrequested insights to the world…

Austin, TX, June 9, 2026

I love my son. Well, I love all my kids of course, but today, I am talking about my recent LSU graduate, hot on the trail of his opening salvo in the worker's world. He is competent, well spoken, dresses sharply and is eminently hirable…. I would never recommend making him CEO, making him a boss, he has much to learn. And I mentioned, right, he is looking for work, please hire him ☺

Every fancy, agentic agent AI based "thing" makes the LLM the boss. AI is autonomous, AI is in charge. The LLM is in charge of making decisions, planning, accessing "tools" and skills and making use of all this fancy autonomous AI agent infrastructure we are learning about. Autonomous, a boss and in total control. Hmm…

Makes me think of the Rush classic, Working Man. Rush highlighted the drudgery of the worker. Clearly in the agentic AI world, the agent is promoted, moved beyond the realities of the world Rush describes and given the role as boss, never to have toiled in the work-a-day life of an entry level worker! Oh, what would Neil. Peart think about AI…

In this AI as Boss model, the LLM runs in a harness. The harness is needed as the raw LLM just creates text, it chooses the next word, really really well, but on its own it will not act. So, agentic agents always have a bit of a harness, which is actually software. Code. A program that lightly harnesses what the LLM is doing, lightly indeed. The vast majority of agentic AI agents are a mostly LLM and minimally a software harness.

So the LLM is the Boss, and the harness is the worker!!!

And harnesses are silently growing. Every new LLM AI model improves in its ability to reason, think, complete a task etc. We all see the benchmarks and they are getting better. Underneath the sheets, something else is happening in parallel, the models are increasingly using the "harness" more and more, software is doing more of the job. So as capability increases, as the stakes increase when we deploy an AI agent to a more sensitive task, the harness grows…

Now, let's get back to my son. He wants to work in a bank. If he is lucky, like many of us, he will get some entry-level role that gets him in the door. For me it was doing quotes

and callbacks at Charles Schwab, buried deep inside a branch in Sunnyvale, never to see actual customers. Drudgery for sure, but it got me going. I don't think Chuck would have offered to make me a boss, not a CEO or even a supervisor of other people. Nope, never was gonna happen…

And when my son lands at a bank (after one of you hires him), he will surely not be given the keys to the wire transfer room and told he is in charge, not gonna happen… He will be seen for what he is, a raw ball of talent just awaiting guidance and supervision, able and willing to prove himself, but definitely not the boss.

So why do we make the LLM the boss? Why do we give an LLM that is new to its job all the reins? Why are we giving the LLM the keys to the wire room?

Because. Just because. ☺ The entire agentic model rests on the theory of autonomy and for those using an LLM day to day, it is pure theory. What we know today, what I experience every day, is witnessing the AI fail on the first step. It is not capable of completing work on its own. It needs constant verification to get results. It is not the boss. The "harness", the software is the boss, and the person running the agent, they are the boss! For me, the LLM is a worker.

Ah, here is the thing. There is an alternative model. Software in charge and LLM as a sub-routine. The harness grows to be the boss and the LLM becomes the worker. Inversion. In this model, the deterministic software leads, I call these pieces of glory "deterministic software agents". They are LLM enabled and the software harness is the boss.

There is an abundance of evidence now that the LLM as boss model is being challenged by the reality of deployment. In other words, autonomous LLM agents don't work, they can't complete work at a high rate of reliability. Well, they can sort your email in-box, and they can write a first draft of a killer research paper (make sure to check the sources) and they can even answer a customer's question, some of the basic ones at least, but they are really challenged at doing meaningful work that requires any kind of iteration and following a process. The LLM can do the work, but not reliably. Scott Cook, founder of Intuit used to tell us a task must be 95% accurate to be generally accepted (19-20 correct responses) when he talked about new features. We are far from the 95% standard when we look at AI agents' efficacy…

I don't need to debate this. I wish it were otherwise. Every hour of every day I use AI in a mode called "trustless verification". I assume the AI will fail and I act accordingly. In fact, when I write my DSA agents, the LLM AI piece is usually less than 5% of the overall software logic. 95% software, 5% LLM. This is my reality, I trust not in the LLM magic machine…

So, the real question seems to be the ratio, how much is software and how much is the LLM? That frames the discussion the right way. We can now decide on ratio based on the capability. Let the debate rage!!!

One other interesting finding. I recently did an exhaustive review of the AI governance space and looked at the vendors. They all start with the premise of an autonomous agent, and guess what, the LLM boss needs a ton of governance, go figure!!! The LLM boss can't be trusted so this huge category of software now exists, there were 90+ vendors in the category of AI governance, at some point we just stopped counting and reviewing vendors, talk about a saturated category. And all of them are there to harness the LLM as Boss. They are treating the symptom, when the actual issue is the way the agents are being built.

What's next? Who knows. All I know is I am deploying effective DSAs. I am putting into production working LLM software, where the software is the boss and the LLM is the worker. I stay focused on delivery and reality, leave the hype behind…

Look, the AI labs are filled with super smart people, they are making LLM models better, they are also building a bigger harness. I continue to hope and pray that the LLM does in fact get better and eventually become a boss-like capability, but I am not holding my breath. Maybe the upcoming trillion-dollar capital events by the LLM labs will solve this, that's it, throw more compute and hardware at the problem, that will solve it!!!

Let's keep an eye on what they build vs the hype of their IPO-driven PR machine… The proof is in the taste of the puddin!!!

I noted recently the LLM harnesses are starting to have the LLM verify, that is the right impulse, as I mentioned I verify constantly after a single step. I wonder if the agentic companies know the LLM can't self-verify reliably. Turns out the LLM will tell you it verified, it might not have even bothered to check, and when it does check, it will hallucinate results. The actual method which works, external verification. A second, different LLM model can verify and get reliable findings and of course, the person verifies as well. Trusting the LLM to verify is a rookie mistake, the LLM labs will I am sure figure this out quickly.

The future is clearly gonna be dominated by AI. The question is LLM as boss or worker and right now, the answer is clearly, worker. So, go out there and experiment, write some software, couple it with the LLM machine and watch the awesome results. AI as a force-multiplying effect on output and abundance of everything, this is the way. And, again, any entry level offers for my son, please send em my way, always a supportive dad and sorry Timmy for using you as my foil in the Fintagonist universe.