The Eternal Battle Between Open and Closed Systems

FEB 08, 2025 • PAID

In the grand sweep of human technological evolution, we repeatedly witness a fascinating pattern: the tension between open and closed systems, between the w frontier of public infrastructure and the controlled confines of private domains. pattern has manifested itself across multiple technological revolutions, from the internet to blockchain to artificial intelligence, revealing a deeper truth about h humans adopt transformative technologies.

Consider the birth of the internet. In its early days during the 1990s, many corporations viewed the public internet with deep suspicion. Their concerns we entirely unfounded – here was a wild, uncontrolled network where anyone could potentially access sensitive information. The natural corporate response was to r into the familiar comfort of intranets: private, controlled networks that promise security and predictability.

These corporate intranets seemed like the perfect solution. They offered email, f sharing, and internal websites, all within a carefully controlled environment. Ma companies invested millions in building these private networks, convinced they represented the future of corporate communication. Industry analysts confident predicted that serious business would always require the security and control of private networks.

But they were missing something fundamental about human nature and the pow open systems.

What these early skeptics failed to grasp was that the true value of a network gr exponentially with its connections – a principle known as Metcalfe's Law. While

intranets could connect hundreds or thousands of employees, the public interne connecting millions, soon to be billions, of people. The sheer innovative potenti this vast network proved irresistible. Developers could create new applications without asking anyone's permission. Ideas could spread and evolve at unprecede speed.

Gradually, then suddenly, the tide turned. The same companies that once shunn public internet began to embrace it. They discovered that the benefits of connec to this vast, open network far outweighed the risks. Security concerns were addr through encryption and other technologies rather than isolation. By the early 20 the corporate intranet had largely become an adjunct to the public internet rath than an alternative to it.

A decade later, history began to rhyme with the emergence of blockchain techno

When Bitcoin appeared in 2009, followed by Ethereum in 2015, the corporate w reaction was strikingly familiar. Once again, the initial response was skepticism, particularly around security and control. And once again, the proposed solution to create private, permissioned blockchains that would offer the benefits of the technology while maintaining corporate control.

Conferences filled with presentations about private blockchain initiatives. Consortium after consortium formed to develop closed blockchain systems. Companies spent millions on private blockchain pilots, convinced that no seriou business would ever trust a public blockchain network.

But just as with the internet, this view fundamentally misunderstood the power open systems. Public blockchains offered something private ones couldn't: true neutrality, permissionless innovation, and network effects that grew stronger wi each new participant. While private blockchains struggled to find compelling us cases beyond the obvious, public networks like Ethereum became hotbeds of innovation, spawning entire new industries like DeFi and NFTs.

By the early 2020s, the pattern was clear. Public blockchains had won the adopti race, with even major financial institutions beginning to embrace them. Private

blockchains, while not disappearing entirely, had been relegated to niche uses, n
like the corporate intranet before them.

Now, in 2025, we're witnessing the same pattern unfold once again with artificia
intelligence. As large language models and other AI systems become increasingl
powerful, many organizations are instinctively retreating to the familiar pattern:
building private, "enterprise AI" models that promise greater control and securi

The arguments are familiar to students of technological history: public AI mode
might leak sensitive data, they can't be trusted with proprietary information, the
need to be carefully controlled. Just as with intranets and private blockchains,
millions are being invested in building closed AI systems that promise to offer tl
benefits of the technology while maintaining strict corporate control.

But if history is any guide, this too shall pass. The fundamental advantages of op
systems – network effects, permissionless innovation, and rapid evolution throug
broad usage – are likely to prove decisive once again. Public AI models, trained o
vast amounts of diverse data and improved through billions of interactions, will
develop capabilities that closed, enterprise models simply cannot match.

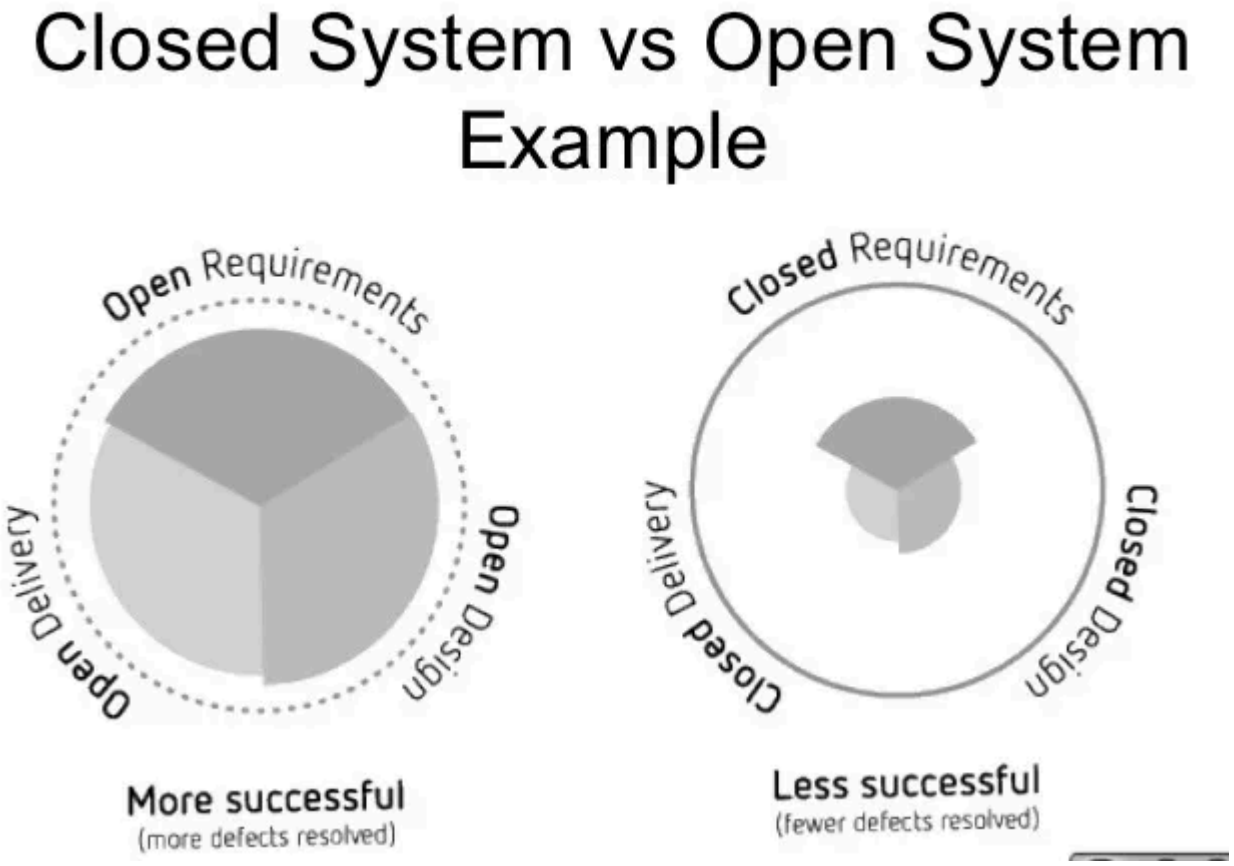
The future may well see a similar pattern to what we observed with the internet:
organizations learning to manage the risks of public AI systems rather than avoi
them entirely. Just as companies eventually learned to secure their internet prese
through firewalls and encryption rather than retreating to intranets, they will lik
develop ways to safely leverage public AI while protecting sensitive information.

The enterprise AI models of today may well follow the path of corporate intrane
private blockchains – not disappearing entirely, but becoming specialized tools r
than the primary way organizations interact with the technology. The real innova
the transformative developments, will likely happen on public systems that can
harness the collective intelligence and creativity of millions of users.

This pattern – from skepticism to private alternatives to eventual embrace of pu
systems – appears to be a fundamental aspect of how human societies adopt
transformative technologies. It reflects our natural tension between the desire fo

control and the need for innovation, between security and possibility. Time and the mathematics of network effects proves decisive, driving us toward open syste despite our initial resistance.

As we stand at the dawn of the AI age, we would do well to remember these lesso from history. The future rarely belongs to closed systems, no matter how secure sensible they might seem at first. The real revolution, as always, will likely come the open frontier where innovation knows no bounds.



← Previous

Nex

Discussion about this post

Comments Restacks

Write a comment...