Immunology for the Internet Age

~lagrev-nocfep

IN THE BEGINNING, *God created the prokaryotes. And the prokaryotes were without nucleus and organelle; and structural simplicity was upon the face of the deep. And chemotaxis moved it upon the face of the waters.*

A single-celled organism possesses many advantages, notably simplicity of form. Being largely indistinguishable, they have no differentiation or specialization. Prokaryotes often form large colonies, such as the cyanobacteria. Some prokaryotes discovered early on that it paid better to consume resources that had already been processed into usable form by another cell, rather than to process those resources oneself. Thus predator and prey were born, and they have always exemplified divergent evolutionary strategies. The resulting arms race meant that predators were continually adapting to better extract resources from prey, while prey were evolving to evade, resist, fight, or poison predators. Selection pressures applied at individual, species, and clade levels, led to speciation across deep time.

More complex forms seemed better able to evade predators, and thus simple symbiotic alliances between differentiated prokaryotes evolved into the eukaryotes and multicellular life forms. Simpler forms also abounded, including the liminal virus. Evasion of pathogenic disease, or disequilibrated colonization by simpler forms of life, has been a primary driver towards increasing complexity in multicellular life.

The Internet began in the late 1960s, born of alliance between the Cold War Department of Defense and the academic research community. This community had a signal advantage: it possessed strong norms of discourse which shaped the professionalism of the community. The nascent Internet generally functioned as a real-name high-trust environment—if not exactly of peers, at least of colleagues.

The Internet evolved as a coordination mechanism—literally a nervous system incarnate in copper and silicon—particularly through the Usenet days of the 1980s. One hallmark of the Usenet era is a gradually eroding social trust. Spam was invented and Internet-based scams started to spin up. Pseudonymity gained in popularity as a countermeasure to both of these as well as restrictions on discourse. The revelation that persistent digital records could cost real-world reputation further fueled a cyberpunk obsession with identity control and hacking.

~lagrev-nocfep, “Immunology for the Internet Age”. *Mormon Transhumanist Association Conference (MTAConf) “Decentralization of Power”.* ~2022.3.19..09.30.00.

Computer viruses could propagate for the first time. Although von Neumann and others explored the possibility of mathematical structures which could self-replicate, it was not until the Creeper virus in the 1970s that self-replicating code was observed in the wild. Like a bacillus in an immune system-free host, code-based computer viruses began to spread from the 1980s onwards.

The crisis arrived in the form of the World Wide Web. Founded initially on a belief in the democratization of information, the Web rapidly became dominated by a handful of large corporations. User experience became the predominant driver of adoption, leading to rapid preference cascades as new platforms became available. Any child of the 90s or earlier can recite the lived litany: Ebay, MySpace, Friendster. Initially these served as proofs-of-concept, then became the only significant player, at least until the next killer app came along. Search engines drove discovery, then focused attention asymmetrically. The "walled garden" approach of AOL, then Apple and Facebook, led to concentrations of users which tipped the balance from single webpage hosts presenting their own idiosyncratic views to corporate-approved genericity and ultimately censorship.

As Internet data sources have overwhelmed traditional media, publishing, and distribution, the resulting tsunami of information and informatization has swept into every corner of lived human experience in technological societies. The ongoing universal exposure to alien and internally incoherent value systems has undergirded the well-documented crisis of credibility (or collapse of meaning) that all Western institutions are experiencing today. The World Wide Web and its technological predecessors acted as a cultural petri dish of clean agar, which grew every spore and germ which fell upon it.

The turn towards a low-trust then zero-trust environment was inevitable if anything like an analogy with prokaryotic evolution holds true. Megacorp platforms are in a way worse than a purely zero-trust environment, because they don't advertise that the world is zero-trust. They lure the unwary into transgressing arbitrary global norms and courting the wrath of social media mobs and the concomitant loss of access to their data held in "trust." The pre-Web cypherpunks were right: "Privacy is the power to selectively reveal oneself to the world." If anything, they were too narrow; not only their valued crypto-anarchic "open society" but *any* non-megacorp society at all requires true privacy.

High culture and low culture have both articulated and preserved valuable insights and forms of human flourishing. However, throughout the 20th century and particularly by means of the consumer revolution, our lives have been thoroughly colonized by capital and commercial instruments. So-called "economies of scale" have disrupted smallholders, artisans, and shopkeepers to the extent that these have been virtually eradicated from the modern landscape in favor of the plastic and polluting "dark Satanic mills." Although small-scale "provident living" has supported gardening, canning, and home production, none of this has survived across a large enough cultural segment to matter macroscopically, and it has unfortunately been tarred with the "prepper" brush that delegitimizes economic downsizing as antisocial because anticapitalist. Not only have physical goods entered a post-consumer phase, but only certain ideas, attitudes, political stances, regional accents, and sensibilities enjoy the sanction of megacorp sociality. There is essentially no native culture left, only that forged in the brand management office.

What cyberspace (and human culture writ broadly) needed was an immune system—and in good Darwinian form, such an immune system has been evolving before our eyes. An immune system formally consists of layers with increasing specificity: first surface barriers, then the innate immune system, and finally the adaptive immune system. The objective of the immune system is to protect the organism: in this case, human sociality and agency.

In an immune system, *surface barriers* are designed to make it hard for exogenous agents to enter a cell or organism; in our analogy, the primary surface barrier was the match of physical separation to psychological separation. Surface barriers were rendered finally obsolete by the launch of the World Wide Web and its subsequent infiltration of every aspect of human culture. To the extent they exist today, it is a matter of ignorance, self-discipline, or happy accident.

The *innate immune system* responds non-specifically to pathogens. Any immune system must have a way of deciding what is *me* and what is *not-me*. Framed as an identity problem in a zero-trust environment, users have evolved several ways to uniquely identify agents without reference to legacy systems. Chief among these means is the blockchain, introduced by Bitcoin for control and transaction of digital assets and since much exploited beyond its design intent.

Identity is still fluid and polysemous, but it is also indelibly demonstrable. The individual actor has the capability to express itself with many public faces or none; one of these typically enjoys government sanction and liability, but it is no more *real* than the others, only more legible to regulation and taxation.

Another aspect of the innate immune system is the public visibility of code. Open source has developed an ethic of transparency on epistemological and practical grounds. (You have a right to know and change what code you are running, and errors are more likely to be detected by many eyes.)

The *adaptive immune system* responds to specific pathogenic incursions. Particular conditions arise, whether through social, regulatory, military, or other requirements, which must be met with specialized forms that are thereafter in evolutionary competition with the external factor. For instance, one megacorp solution to what it perceives as a threat, i.e. unsanctioned memes, is to attempt to mandate the ultimate traceability of any image's provenance. The Internet immune system thus evolves to further obfuscate legibility and enhance individual control and self-determination by shifting to less-traceable technologies such as the InterPlanetary File System. The point is not whether or not a salient technology such as deepfakes, 3D-printed firearms, deviant scientific or political thought, or even the DRM-free sharing of copyrighted material can be contained; the experience with export-grade cryptography has already shown that regulatory attempts ultimately fail. The philosophical question is what kind of world will evolve, a *fait accompli* driven by factors beyond any office or individual. The practical question is how any particular group of actors can preserve their own agency, autonomy, and ambit of action.

The first decentralized autonomous organization, "The DAO" (Đ) itself, was created in 2016 as a way of distributing ownership and stake in a joint venture capital fund. Đ was a new form of organization in that it was essentially a mathematical entity, a set of smart contracts on the blockchain to which anyone had access. Đ lived up at least to "decentralized" and "autonomous." No money was held centrally, with token-based authentication yielding the right to vote on projects. Having set the criteria for membership and investment, Đ then operated in truly democratic fashion until an exploit of imperfectly written smart contract code led to theft, crisis, and the reorganization of the Ethereum blockchain itself.

DAOs have rapidly evolved as a way of distributing ownership and stake in a purely democratic way. The word "democracy" has been much abused, but here I use it in a sense much like the Greek original: the holders of an immutable and indelible token cast their secured votes to govern their *polis*. DAOs represent a resurgence of the sovereign city-state in new guise. Will this be enough to evade "imperial" aggregates which dominate today's Web?

Decentralized autonomous organizations, zero-knowledge cryptographic proofs, cryptocurrencies, proof-of-identity systems, and their as-yet-unborn kin represent the evolution of an immune system on top of the Darwinian churn of the legacy Internet. The stakes are necessarily high: possession is *de facto* ownership, the other end of the stick from "not your keys, not your coins." The focus is currently on ownership of money, non-fungible tokens, and similar assets, but broadly speaking such systems allow the authenticated ownership of all data and assets one holds, from chat messages to market shares to physical real estate. There may be good reasons to retain the legacy system for some classes of physical or legal artifacts, but at minimum these will be in competition with purely autonomous constructs. "Code is law."

Having set the criteria for membership, a DAO can act as the stakeholders direct. The form is still somewhat "yeasty" in that like cyanobacteria it acts as an undifferentiated mass, and we should expect further innovations in DAO-like entities. The most salient epithet of a DAO is "decentralized"; one can imagine hierarchical, concentric, or role-specialized DAOs as well as other taxonomically related forms, just as one can imagine progressively less organized instances in a chaos-happy Internet.

Blockchains and DAOs operate as proof-of-work, proof-of-stake, etc. This provides node operators with a way of verifying consensus reality and cementing a record of digital transactions. Future innovations hold forth the possibility of secure proof-of-identity blockchains, wherein each node which can provide concrete cryptographic evidence of its identity gets a vote on the consensus.

We must consider modern systems to necessarily interact at the pinnacle intensity of competence and competition: any differential advantage that can be exploited to outcompete an adversary not only can be exploited but *should* be. Any system which does not have an operational DAO-like layer is immunocompromised. All tools for the individual and collective need to be architected around a zero-trust adversarial world. They also need to guard the embers of community and enable new growth.

In a nutshell, the early Internet was a cocktail party. By the age of Usenet and the World Wide Web era, the Internet evolved into a player-versus-player defect–defect equilibrium in which brigading, spamming, and anonymity are rational adaptive behaviors. Indeed, anonymity is barely a protection given the lengths to which governments and megacorps go to prevent truly untraceable usage. The agencies have given up on any other model of reality, lacking a vision of humanity other than as atomized krill for megacorp apex predators. The legacy megacorp Internet has become a crab bucket, always drawing everything back into itself in a dysfunctional and frankly satanic way.

Communities built on decentralized Web3 platforms such as Mastodon, Fediverse, and Urbit have stepped back from the purely PvP world of the globally-namespaced social media Internet. These today have more of a block party feel, wherein one can wander from house to house and encounter some of the same faces in the same or new guise. Conversations can drop and resume anew in very different locales with largely the same composition. Marrying the underlying cryptographic identity requirements of DAOs to communication tools and databases yields a strong stable solution to the problem of retaining a foothold of personal identity from which to coordinate one's multifaceted digital life. IPFS, Sovrin Foundation, Tim Berners-Lee's Solid, and Urbit all offer their take on this requirement. Even a Signal chat group running its own server is a kind of tokenless DAO.

The *telos* of social computing is to recreate the village green, not the penitentiary. Revisiting a thesis from above: "All tools for the individual and collective need to be architected around *using cryptographic proofs to create stable high-trust havens* in an otherwise zero-trust adversarial world." The village is a stable, long-term tribe which shares values and assets in common, from which a member occasionally ventures out into the broader social web but always has a home. Every village will grow its own culture, perhaps even its own *cultus*, enabled by decentralized technologies to protect their assets and precious peculiarities. The World Wide Web has been an extinction-level event for many forms of life, livelihood, and culture. For others, it has offered strange forms of life support and even thriving. With a new immune system evolved and now operational, human endeavor stands on the cusp of a Cambrian explosion, unconstrainable by a rent-seeking boardroom-and-bureaucracy world that never comprehended the light shining in its darkness.