

# Immunology for the Internet Age

~lagrev-nocfep

*A consideration of the history of the Internet motivates introspection on the nature and causes of social dysfunction in a globally shared space. Centralized solutions fail to yield satisfactory outcomes for human freedom and thriving. Decentralized autonomous organizations and their technological apparatus together represent the evolution of an immune system against a corporatized Internet.*

[illegible]

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 competitive 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, lead 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 (yielding specialized features such as the nucleus and mitochondria) and multicellular life forms. Simpler forms also abounded, including the liminal virus. Viruses are forms of near-life so simple that they simply exploit cells to reproduce. They are entirely predatory or at best symbiotic with other life.

Evasion of pathogenic disease, or disequilibrated colonization by simpler forms of life, has been a—if not the—primary driver towards increasing complexity in multicellular life.<sup>1</sup>

The Internet began in the late 1960s, born of scientific alliance between the Cold War Department of Defense and the academic research community.<sup>2</sup> This community had a signal advantage over many subsequent communities: it was dominated by strong norms of discourse which shaped the professionalism of the community. This is not to discount the significance of courtly intrigue, of course, which deftly exploited tensions between competing systems.<sup>3,4,5</sup> Throughout this era, though, the 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. In our days of heightened online tension and mediated preference cascades, it is rather quaint to go back and look at what qualified as email flame wars at the time (e.g. Torvalds/Tanenbaum). One hallmark of the Usenet era, however, is a gradually eroding social trust: spam was invented<sup>6</sup> 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 someone's job<sup>7</sup> further fueled a cyberpunk-like obsession with identity control and hacking.

---

1 Kaufman, Jim. (2010) [“Evolution and immunity”](#). *Immunology* 130, iss. 4, pp. 459–462.

2 President Eisenhower's original coinage was likely “the military-industrial-academic complex.”

3 E.g., Richard Bellman of the RAND Corporation on the origin of “dynamic programming,” a mathematical discipline: in dealing with a recalcitrant secretary of defense who hated the word “research,” Bellman instead chose the word “dynamic” arbitrarily because “it's impossible to use the word ‘dynamic’ in a pejorative sense. ... It was something not even a Congressman could object to. So I used it as an umbrella for my activities.” (Bellman, Richard. (1984) [Eye of the Hurricane](#).)

4 The nuclear triad doctrine, joining the Air Force's Strategic Air Command bombers, the Navy's nuclear submarines, and the Army's ICBMs and other assorted nuclear warheads, was based less on strategic considerations than on appeasing constituent departments of the military. Strategists developed a formal justification decades later in a magnificent demonstration of motivated reasoning. (Woolf, Amy. (2016) “U.S. Strategic Nuclear Forces: Background, Developments, and Issues”. [CRS 7-5700](#).)

5 The Air Force early commissioned the RAND Corporation on contract with Douglas Aircraft Company as the first “think tank”; RAND soon upended the traditional role of passive reception of studies by making its own recommendations and showing their analytical chops. Other service branches followed suit, such as the U.S. Navy's Center for Naval Analyses and the Battelle Memorial Institute for various federal contracting agencies; compare also the role of the national laboratory system, e.g. Los Alamos, Sandia, Livermore, etc. for the Department of Energy and Department of Defense. (Rich, Michael. (2003) “RAND: How Think Tanks Interact with the Military”. [RP-1050](#).)

6 “On January 18, 1994, the first large-scale deliberate USENET spam occurred. A message with the subject “Global Alert for All: Jesus is Coming Soon” was cross-posted to every available newsgroup.” ([Wikipedia, “History of email spam”](#))

7 The first instance which seems to have brought this to general public awareness was the submission of Judge Robert Bork's video rental history as evidence in his Supreme Court hearings before the U.S. Senate. The resulting Video Privacy Protection Act was delightfully naïve. Besides relying on “video rental” narrowly construed, users have effectively no leverage against unilaterally-imposed terms of service and end-user license agreements. (See, e.g., [Electronic Privacy Information Center, “Video Privacy Protection Act”](#).)

Computer viruses could propagate for the first time: it never made much sense to build a computer virus until systems were connected. Although John von Neumann and others early explored the possibility of mathematical or code structures which could self-replicate, it was not until the Creeper virus in the 1970s that self-replicating code was observed in the wild. And 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 (henceforth “megacorps”). 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 (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.<sup>8</sup>

---

When was the first time you did something in the physical world because of something you read or encountered online? For generations born after the advent of the Web, they may not recall such a time when meatspace existence wasn’t driven by life online. As Internet data sources have overwhelmed traditional media, publishing, and distribution services, the resulting tsunami of information and informatization has swept into every corner of lived human experience in technological societies. The psychological (memetic) virus problem is much greater than actual code viruses. The ongoing universal exposure to alien and internally incoherent value systems has undergirded the well-documented crisis of credibility (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. We live in the midst of a memetic epidemic because of the World Wide Web, and the dominant strain is corporate, approved by a marketing department and run through a search-engine optimization algorithm.

---

8 E.g. Tumblr and OnlyFans and adult content; Twitter and right-wing content; Youtube and Facebook and unsanctioned medical content, etc. Note that this is regardless of the viability of a given view or the necessity of vigorous debate within a field, but focuses on the palatability of politics to the megacorp entity providing the platform, even if the content drives platform usage.

If we reason analogically to a biological ecosystem, then the medical guild systematically reveals its preference for pharmaceutical-grade interventions to treat medicalized conditions. Any condition deemed adverse will sooner or later have its own expensive patented drug. Medical pharmaceuticals are of mixed efficacy both theoretically and practically<sup>9</sup>; worse than this, megacorp ‘cures’ are at best as bad as the disease.

The turn towards a low-trust then zero-trust environment was inevitable if anything like an analogy with prokaryotic evolution holds true. The megacorp platforms are in a way worse than a purely zero-trust environment, because they don’t advertise that the world is zero-trust. Thereby 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.” To mix a metaphor, megacorps are apex predators—at best, sheepdogs with a strong strain of wolfishness; at worst, tar pits manned by various bad-faith actors. The pre-Web cypherpunks were right: “Privacy is the power to selectively reveal oneself to the world.”<sup>10</sup> If anything, they were too narrow; not only their valued “open society” (polyvalent crypto-anarchy) but *any* non-megacorp society at all requires true privacy.

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.

First, what is human sociality? Human culture has been the means of participating in the Great Discussion which ranges from the earliest days of oral culture to the birth of literacy and libraries down to our day. High culture and low culture have both articulated and preserved valuable insights and forms of human flourishing. However, throughout the 20<sup>th</sup> century and particularly by the 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. The siren call of cheap consumer goods has ushered in a generational collapse in self-sufficiency and resulted in the complete colonization of

---

9 C.f. Stegenga, Jacob. (2016) *Medical Nihilism*.

10 Hughes, Eric. (1993) [\*A Cypherpunk's Manifesto\*](#).

entertainment, food consumption, and self-care by massive corporate brands. Not only have physical goods entered a post-consumer phase, but only certain classes of 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.<sup>11</sup>

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. Ethereum-based ERC tokens represent tweaks of this identity concept, as do many other blockchain platforms.

Identity is still fluid and polysemous, but in certain key instances it is indelibly demonstrable.<sup>12</sup> 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.<sup>13</sup>

Another aspect of the innate immune system is the public visibility of code. Open source has developed an ethic of transparency on epistemological grounds (i.e. you have a right to know

- 
- 11 The mass shift to remote work from March 2020 onwards due to the COVID-19 pandemic has accelerated the trend of corporate colonization of private spaces. At first, this was occasionally humorous, as when a child ran into the background of a Zoom call, or underwear or private materials were inadvertently left in view of the remote audience. In the end, it demanded that individuals reconfigure their homes to accommodate mass corporate preferences, thus another invasion of private space by the megacorp panopticon. I note as well an invasive doctrine demanding “truth in communication” under names like [“radical transparency”](#) and [“radical candor”](#) put forward by partisans of power over against vulnerable employees, clients, and customers, who may be disproportionately affected by a megacorp demand for one-sided transparency. Ultimately, despite megacorp hand-wringing over worker productivity, the fact that remote workers feel comfortable living lives with a bit of “extracurricular activity” means that they are *de facto* carving out private space once again, a heartening prospect—even if pornography usage and alcohol and media consumption are coping mechanisms for dystopia. (Kelly, Jack. (2021) [“Study Shows People Working From Home Are Having Sex, Dating, Taking Naps And Doing Side Hustles On Company Time”](#))
- 12 Several have pointed to the failure of Craig S. Wright to demonstrate cryptographically that he is Satoshi Nakamoto, the pseudonymous inventor of Bitcoin. (C.f. Khaosan, Venzen. (2016) [“Craig Wright is Not Satoshi Nakamoto—The Technical Proof”](#).)
- 13 Davidson, Dale, and Rees-Mogg, William. (1999) *The Sovereign Individual: Mastering the Transition to the Information Age*.

what code you are running) and practical grounds. (Linus's law: "given enough eyeballs, all bugs are shallow."<sup>14</sup>)

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.<sup>15</sup> 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 (IPFS). The point is not whether or not a salient technology such as deepfakes, 3D-printed firearms, deviant scientific or political thought<sup>16</sup>, or even the DRM-free sharing of copyrighted material can be contained<sup>17</sup>; the experience with export-grade cryptography<sup>18</sup> 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 individual or office) and 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" (Ð) itself<sup>19</sup>, was created in 2016 as a way of distributing ownership and stake in a joint venture capital fund. Ð 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. Ð 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, Ð 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.

---

14 Raymond, Eric. (1999) [\*The Cathedral and the Bazaar\*](#).

15 The [Coalition for Content Provenance and Authenticity](#) "addresses the prevalence of misleading information online through the development of technical standards for certifying the source and history (or provenance) of media content."

16 Cf. Walker, Shawn, et al. (2019) "[The disinformation landscape and the lockdown of social platforms.](#)" *Information, Communication & Society* 22, pp. 1531–43. Walker et al. lament that "highly ephemeral mis/disinformation campaigns" are not susceptible of study due to closed platform APIs. "Social media platforms [attempt] to rekindle trust by appearing to reinforce individual privacy within a newly secured user community, a set of measures that also locked academic and non-profit researchers out from studying social platforms while preserving corporate and business access to social media users' data." They fail to address the tension between community self-determination and academic exploitation.

17 "If in fact you can't crack [the encryption] at all, government can't get in, then everybody is walking around with a Swiss bank account in their pocket – right? So there has to be some concession to the need to be able to get into that information somehow." ([Barack Obama in March 2016 at SXSW](#))

18 Heninger, Nadia. (2016) "[The Legacy of Export-Grade Cryptography in the 21<sup>st</sup> Century](#)".

19 Chohan, Usman. (2017) "[The Decentralized Autonomous Organization and Governance Issues](#)". Discussion Paper Series: *Notes on the 21<sup>st</sup> Century*.

While the heirs of Ð serve a role in the current Internet immune system, the original was formed in response to exogenous regulatory concerns, notably ongoing governmental insistence on restricting investment to the already-wealthy.<sup>20</sup> The U.S. Securities and Exchange Commission and other agencies have in place arbitrary investor requirements which would make little sense even if pegged to something like inflation or index rather than the rapidly-devaluing petrodollar. Nominally put in place to protect the naïve from getting scammed, these restrictions have had the pernicious effect of pulling up the ladder behind the *actuel riche*.

DAOs have rapidly evolved as a way of distributing ownership and stake in a purely democratic way. (As an aside, 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 society.) 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 old cryptocurrency chestnut). 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. (As an aside, I am of the philosophical opinion that legal recognition should not be sought generally for new forms of organization, as any legibility to legacy systems opens new attack surfaces in an immunological sense.) “Code is law.”<sup>21</sup>

A decentralized autonomous organization seems to be at least the first two: having set the criteria for membership, the organization can act as the (distributed<sup>22</sup>, possibly unknown in the zero-knowledge proof sense) stakeholders direct. This 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.<sup>23</sup> 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.

---

20 Idle speculation wonders how Joseph Smith and the saints in Kirtland would have fared with a DAO-secured altcoin rather than the Kirtland Safety Society’s anti-banking company.

21 Lessig, Lawrence. (1999) *Code and Other Laws of Cyberspace*.

22 Hobart, Byrne ~lableg~tadrex. (Nov 17, 2021) [“The Promise and Paradox of Decentralization”](#). *The Diff*.

23 See, e.g., the Governor Alpha smart contract protocols. Solari, R. (2021) [“The case for Governor Alpha”](#).



Like the first mutant with a new gene, D itself failed. Many lessons can be drawn from that failure, including the criticality of getting smart contract code absolutely correct (“code is law”), and how to administer a blockchain in the presence of massive fraud. And indeed, what has happened to the blockchain world of decentralized finance? Millisecond differentials in responsiveness lead to huge swings in profitability of transactions. Frontrunner bots watch algorithmically for transactions they can complete faster than the original source, thereby making money on asymmetric knowledge.<sup>24</sup> Zero-day exploits of code abound, heralding a need for more thorough vetting and more expressive and secure smart contract languages.

Blockchains (and thus DAOs via Ethereum) operate as proof-of-work, proof-of-stake, etc. This provides node operators with a way of verifying consensus reality and thereby cementing a record of digital transactions. Future innovations hold forth the possibility of secure proof-of-identity blockchains (such as the Uqbar Layer 1 smart contract blockchain on Urbit<sup>25</sup>), 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. Illegibility, redundancy, and apposite complexity are allies in the immune fight to maintain identity and ownership in the modern Internet.<sup>26</sup> Any system which does not have an operational DAO-like layer is immuno-compromised. 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 into 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. This approach is adaptive for agencies which have given up on any other model of reality, fundamentally lacking a vision of humans as other than atomized individual krill for the megacorp apex predators: consumers for the consumers. The legacy megacorp Internet has become a crab bucket, always drawing everything back into itself in a dysfunctional and frankly satanic way.

---

24 Robinson, D. (2020) “[Ethereum is a dark forest](#)”. Paradigm blog.


25 [Uqbar Network](#); “[Introducing Uqbar Network](#)”; ~hocwyn-tipwex/uqbar-event-horizon (Urbit group)

26 This is not to deny the benefits of system-legibility, in particular legal protections. As common law develops around DAOs, I hope for similar affordances where they must interact with the legacy legal system.



Communities built on decentralized Web3 platforms such as Mastodon, Fediverse, and Urbit<sup>27</sup> 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 or room to room 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 token-free DAO.

Since the Renaissance, essentially all theology has been humanist in nature, concerning itself with how man should live to flourish in this world and inherit in the next. Even secularized descendants enjoin an ethos of ritual behaviors and practices. The social and cultural "stack" (in software parlance) upon which we build provides for a variety, broad or narrow, of human cultural forms. Lately, the variety of forms has been diminishing both by cutting off older forms from the modern world and by cultivating only certain state-legible apex predators<sup>28</sup> and their preferred ovine repast.

Contra this monoculture, 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 well below Dunbar's limit 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. 

---

27 Originally this list included Discord, as there has been substantial growth in stable goal-oriented communities thereon. However, more recently the company [adopted a user policy](#) which subjects use of their product to judgment calls about "off-platform behavior"—a clear violation of a cypherpunk ethos which Discord likely never espoused anyway.

28 E.g., Auerbach, David. (Mar 3, 2022) "[The metaverse will steal your identity](#)". *UnHerd*. Auerbach correctly recognizes and decries the looming "monetisation of identity" which will allow any platform controller to incentivize prosocial or antisocial behaviors at will.