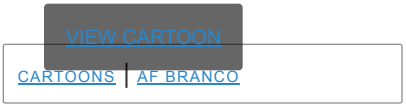
Google's security foibles, its "aggregate and advertise" model, its avoidance of price signals, its silos of customer data, and its visions of machine mind are unlikely to survive the root-and-branch revolution of distributed peer-to-peer technology, which I call the "cryptocosm."

Today, all around us, scores of thousands of engineers and entrepreneurs are contriving a new system of the world that transcends the limits and illusions of the Google realm.

In the Google era, the prime rule of the Internet is "Communications first." That means everything is free to be copied, moved, and mutated. While most of us welcome "free" on the understanding that it means "no charge," what we really want is to get what we ordered rather than what the authority chooses to provide. In practice, "free" means insecure, amorphous, unmoored, and changeable from the top. This communications-first principle served us well for many years.

The Internet is a giant asynchronous replicator that communicates by copying. Regulating all property rights in the information economy are the copy-master kings, chiefly at Google.

In this system, security is a function of the network, applied from the top, rather than a property of the device and its owner. So everything rises to the top, the Googleplex, which achieves its speed and efficiency by treating its users as if they were making random choices. That's the essence of the mathematical model behind their search engine. You are a random function of Google.



But you are not random; you are a unique genetic entity that can- not be factored back into an egg and a sperm. You are unbreakably encrypted by biology. These asymmetrical natural codes are the ruling model and metaphor for enduring security. You start by defining not the goal but the ground state. Before you build the function or the structure, you build the foundation. It is the ultimate non-random reality. The ground state is you.

1. Utterly different from Google's rule of communications first is the law of the Cryptocosm. The first rule is the barn-door law: "Security first." Security is not a procedure or a mechanism; it is an architecture. Its keys and doors, walls and channels, roofs and windows define property and privacy at the device-level. They determine who can go where and do

what. Security cannot be retrofitted, patched, or improvised from above.

For you, security means not some average level of surveillance at the network level but the safety of your own identity, your own device, and your own property. You occupy and control a specific time and space. You cannot be blended or averaged. Just as you are part of a biological ledger, inscribed through time in DNA codes and irreversible by outside power, your properties and transactions compose an immutable ledger. Just as you are bound in time, every entry in the cryptocosmic ledger is timestamped.

---

2. The second rule of the cryptocosm derives from the first: “Centralization is not safe.” Secure positions are decentralized ones, as human minds and DNA code are decentralized. Darwin’s mistake, and Google’s today, is to imagine that identity is a blend rather than a code—that machines can be a singularity, but human beings are random outcomes.

Centralization tells thieves what digital assets are most valuable and where they are. It solves their most difficult problems. Unless power and information are distributed throughout the system peer to peer, they are vulnerable to manipulation and theft from the blenders at the top.

3. The third rule is “Safety last.”1 Unless the architecture achieves its desired goals, safety and security are irrelevant. Security is a crucial asset of a functional system. Requiring the system to be safe at every step of construction results in a kludge: a machine too complex to use.

4. The fourth rule is “Nothing is free. This rule is fundamental to human dignity and worth. Capitalism requires companies to serve their customers and to accept their proof of work, which is money.

Banishing money, companies devalue their customers.

5. The fifth rule is “Time is the final measure of cost.” Time is what remains scarce when all else becomes abundant: the speed of light and the span of life. The scarcity of time trumps an abundance of money.

6. The sixth rule: “Stable money endows humans with dignity and control.” Stable money reflects the scarcity of time.

Without stable money, an economy is governed only by time and power.

7. The seventh rule is the “asymmetry law,” reproducing biological asymmetry. A message coded by a public key can be decrypted only by the private key, but the private key cannot be calculated from the public key. Asymmetric codes that are prohibitively difficult to break but easy to verify give power to the people. By contrast, symmetrical encryption gives power to the owners of the most costly computers.

8. The eighth rule is “Private keys rule.” They are what is secure. They cannot be blended or changed from on top any more than your DNA can be changed or blended from above.

9. The ninth rule is “Private keys are held by individual human beings, not by governments or Google.” Private keys enforce property rights and identities. In a challenge-response interaction, the challenger takes the public key and encrypts a message. The private responder proves identity by decrypting, amending, and returning the message encrypted anew with his private key. This process is a digital signature. By decrypting the new message with a public key, the final recipient is assured that the sender is who he says he is. The document has been digitally signed.

Ownership of private keys distributes power. The owner of a private key (id) can always respond to a challenge by proving ownership of the identity of a public address and the contents of a public ledger. Thus, in response to government claims and charges, the owner of the private key can prove his work and his record. By signing with a private key, the owner can always prove title to an item of property defined by a public key on a digital ledger.

10. The tenth rule is “Behind every private key and its public key is the human interpreter.” A focus on individual human beings makes meaningful security.

How will your experience of the world change when these ten rules define the new system?

Google is hierarchical. Life after Google will be heterarchical. Google is top-down. Life after Google will be bottom-up. Google rules by the insecurity of all the lower layers in the stack. A porous stack enables the money and power to be sucked up to the top. In life after Google, a secure ground state in the individual human being, registered and timestamped in a digital ledger, will prevent this suction of hierarchical power.

Whereas Google now controls your information and uses it free of charge, you will be master of your own information and charge for it freely. Try the Brave Browser of Brendan Eich, formerly of Mozilla and the author of Javascript. It gives you power over your data and enables you to charge for them.

Whereas Google envisages an era of machine dominance through artificial intelligence, you will rule your machines, and they will serve you as intelligent, willing slaves. You will be the "oracle" that programs your life and dictates to your tools.

Whereas Google's "free world" tries to escape the laws of scarcity and the webs of price, you will live in a world brimming with information on the real costs and most efficient availabilities of what you want and need. The proof of your work will trump the claims of top-down speed and hierarchical power. The crude imperatives of "free" will give way to the calibrated voluntary exchanges of free markets and micropayments.

Whereas the Google world strains you through sieves of diversity and runs you through blenders of conformity, the new world will subsist on the foundational realities of individual uniqueness and choice. Whereas the Google world is stifling entrepreneurs' access to the public markets through initial public offerings, which are down 90 percent in two decades, the new world will offer an array of new paths to enterprise. From initial coin offerings and token issues to crowd- funded projects, new financial devices are already empowering a new generation of entrepreneurs. The queues of abject "unicorns"—privately held start-ups worth a billion dollars or more—outside the merger and acquisition offices of Google and its rivals will be dispersed, replaced by herds of "gazelles" headed for public markets at last.

Whereas Google attempts to capture your eyeballs with ubiquitous advertisements, you will see advertisements at your own volition, when you want them, and you will be paid for your time and attention. Again, Brave is the leader of this movement.

Money is not a magic wand but a measuring stick, not wealth but a gauge of it. Whereas money in the Google era is fodder for a five- trillion-dollar-a-day currency exchange—that's seventy-five times the amount of the world's trade in goods and services—you will command unmediated money that measures value rather than manipulates it. Whereas the

Google world is layered with middlemen and trusted third parties, you will deal directly with others around the globe with scant fees or delays.

Emerging is a peer-to-peer swarm of new forms of direct transactions beyond national borders and new forms of Uber and Airbnb beyond corporate gouges. Whereas the Google world confines you to one place and time and life, the new world will open up new dimensions and options of new life and experience where the only judge is the sovereign you.

Does the promise that human dignity will once again take its place on the Internet and that human beings will be masters of the cryptocosm sound too good to be true?

If these principles are enigmatic today, to explain their sources and ultimate success, we must, as Caltech's Carver Mead tells us, "listen to the technology and find out what it is telling us."