

A Case for ALGORTHMICA

M-Marvin Ken

Reference: -

A personal view of Average-Case complexity by Russell Impagliazzo

Background

There have been many genuflections over what might have caused the current socio-economic and socio-political crises and conundrums the world is facing today, especially with regard to price inflation and the mismatch between technological advancement and livelihood for most people.

For example, the fact that their parents could afford homes while young adults while most millennials and Gen-Z cannot, could be put to ballooning numbers, except most millennials and Gen-Z adults today earn more than their parents did. So the money has a problem. It is not really “more”.

Also, let us blame it for the fact that many young people are now “finding themselves” and identifying as; *actually* of opposite sex, climate propagandist, fat and happy, rage-cultured.

But that doesn’t make sense. What has money to do with any of that stuff?

Well it is never the money per say, but how it moves. Who controls it, how, and to whose benefit.

After WW2, two technological shifts occurred that put us on this path. The first was the invention of highly powerful encryption systems, way better than the German Enigma. The other was the invention of even better centralized computer algorithms that have steadily grown to produce impressive artificial intelligences like [ChatGPT](#), and data-driven defence industry technology that made a [25 year old a billionaire](#), amongst other wonders.

This combination – secrets plus exponentially growing centralized digital intelligence – has put us where we are. It could be an Impagliazzo 6th world all on its own.

In fact, it is. Wonder what we shall name it. Because the ability to have strong encryption – Cryptomania, is now merged with the ability to have very powerful computational capabilities albeit hyper centralized – Centralized Algorithmica.

Note; Our computers today lie more in the realm of Heuristica (they heavily rely on heuristics to solve problems. Especially artificial intelligences) with regard to the way they solve problems, but Impagliazzo says in the average case, linearly growing time constraints make Heuristica just another Algorithmica, i.e., comparing linear growth of complexity with the exponential advantages that come from massive deployment of new technology.

CxCA – Cryptomania x Centra-Algorithmica

This is the world we are in today.

A subtle False belief in More Encryption

Sometime in the late 20th century, people in CxCA felt that the solution to the government eavesdropping on them with their powerful algorithms is to create encryptions that protect them from these algorithms. The government felt pained that people did not want it to look at them all day.

Hence we got Paul Zimmerman and his highly successfully P2P scheme. Meanwhile, RSA was now being deployed in all email correspondence and the rise of the Bitcoin cryptocurrency added ECDSA to its armoury, bolstered by a chain of SHA256 hashes.

The government however had an ace in their hand. They still printed fiat as they pleased and it was, still is, defacto currency nationwide and internationally. This money would find its way into the pockets of billion dollar internet companies usually as tax fee credit and grants, and in return, they still got your data. Freely given during signups and while using Facebook, Instagram, SnapChat, WeChat, Twitter, because human beings cannot help sharing their info with other human beings.

Freely given in TikTok while sharing #lunch #workout #newhouse #vacation reels. If anybody is an avid social media person, AI algorithms today can probably tell what your likes and dislikes are on everything in your daily life. Who your friends are, what you and they like talking about, what businesses they run, what you do all day.

So with our hands, we have encrypted emails, and with our mouths we have given the big owners of Centra-Algorithmica a glimpse into what our emails contain.

In this way, encryption has somewhat failed. And the reason is simple, you and I, broke millennial or Gen-Z young adults, have no productive capital in our hands except our smartphones and laptops. To get ahead, we have to create a lot of digital content, usually revealing ourselves in the process.

If our ventures can get big owners of systems to have even more influence over everyone else, we get multiple rounds of seed investment and retire early. YouTube, WhatsApp, AirBnB, Uber, Reddit, #1 – Google, all have the same thing in common – they bring more people to the big systems. Numbers, views, users, are everything in this game. So much so that direct advertising is not even a revenue source anymore. Just those Gigabytes of data flowing across these free platform conduits everyday is enough. With the power of Centra-Algorithmica, a lot of smart computer scientists have learnt how to turn this data into gold. And they are still learning.

Meanwhile...

The big data owners, via strong encryption like RSA, are protected from you eavesdropping on them. So little useful data flows downhill you'd make exactly zero to negative profits if you tried running a Big Data analytic scheme for celebrities, billionaires and, don't do it, government data. Even if you get the data, it will seem weird and intrusive.

This [young man](#) tried, he didn't make a million dollar startup like he should have.

Destroying CxCA to build a Decentralised Algorithmica

I am a Pacifist at heart, and a Bitcoiner at that. Today is the 16th / 12/2023 and the Bitcoin halving, expected to shoot the price over \$100k, is 4 months away.

Bitcoin however could do with a bigger price boost. If quantum computers somehow got out of the rut they are stuck in, somewhere in the void of great knowledge, we'd have a decentralised algorithmica on our hands.

Hacking RSA is the #1 fear but it is beside the point. If factoring any product of prime numbers, hence if looking for prime numbers, ever got easy, we would revolutionise a lot of technology for the individuals benefit. If $P = NP$, even if for some vital problems alone, we shall transform medicine, manufacturing, cooking with better materials for renewable systems, medical devices, easier agriculture with cheaper tractors for everyone.

Instead of lawnmowers, everybody in the world deserved a cheap futuristic family tractor.

Food is the backbone of everything. If growing food is made child's play, bingo. Apotheosis.

End Note

This is why I pursue Bitcoin x Quantum Computing.

Hacking encryption like RSA may alienate the world into camps of informationally disconnected points (as data flows will not be secure), but it could unleash manufacturing knowledge like nothing seen before.

It is Dune come to life. Except we shall have no need to fight and cut throats for spice melange. The sun gives us more than enough energy and hopefully, quantum computers will tell us how to tap more of it. They will hack the secrets behind energy capture and storage.

Again, hacking encryption is beside the point.

Algorithmica could be our fertile crescent.

P.S. Hacking nukes wherever they sit isn't so bad an idea either. A matured Algorithmica could make the very idea of building a nuke dangerous to the maker. Because your nuke will be hacked, to blow up in your face!