Next Steps for DINRG

Discussion

Background: DINRG Charter

- Investigation of the **root causes of Internet centralization**, and articulation of the impacts of the market economy, architecture and protocol designs, as well as government regulations;
- **Measurement of the Internet centralization** and the consequential societal impacts;
- **Characterization and assessment** of observed Internet centralization;
- **Development of a common terminology and understanding** of (de-)centralization;
- Interaction with the broader research community to explore **new research topics and technical solutions** for decentralized system and application development;
- **Documentation of the outcome** from the above efforts via different means (e.g., research papers and RFCs) as inputs to the broader conversation around centralization; and
- **Facilitation of discussions** between researchers, organizations and individuals involved in Internet standards and regulations.

A quick summary of DINRG email exchange

10/18/2024 – 10/23/2024

Sorting out different issues

Finkhäuser:

- Baran's old RAND memorandum has good definitions of distributed/decentralized with regards to network architectures.

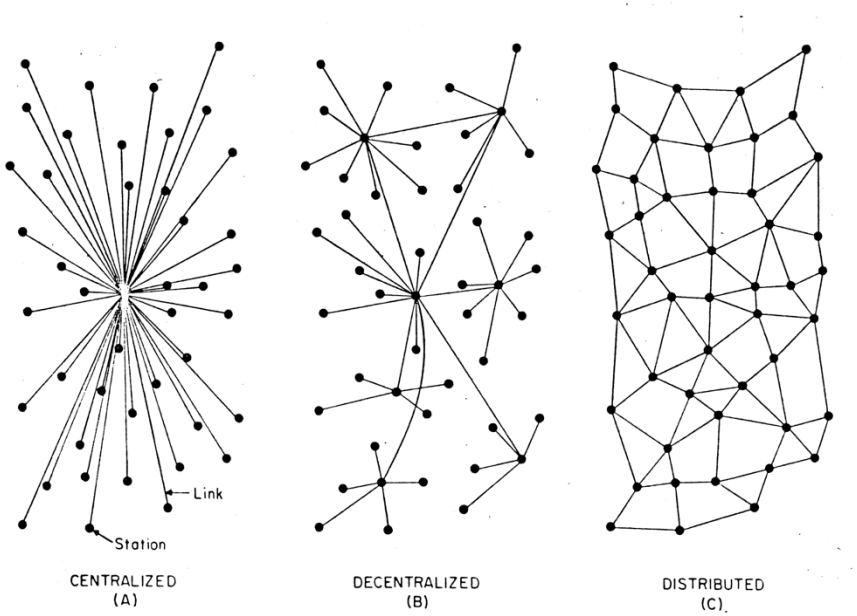

FIG. 1 — Centralized, Decentralized and Distributed Networks

- One should perhaps distinguish between *network architectures* and *control mechanisms*, to avoid this kind of confusion (referring to the discussions of what's/whait's not centralized)

Technical Centralization vs Control Power Centralization

Technical / Physical Centralization

- A system of 100 nodes, claims to be operating in decentralized manner, but 90% of those nodes are VMs are on the same Cloud Provider/same location
- what if 90% of blockchain/cryptocurrency nodes are powered by a single electricity provider?

The above conditions show that the system can be subject to single point of failure

  - independent from what the system is/does (BLT or not)

- The classic economic theory of centralization: the limits to centralization was set by the increased complexity of the ever larger enterprise
  - more agile competitors might compete more efficiently

Another system design example: big size may lead to complexity

Control Power Centralization

- The intention of BLT/Web3: avoid centralized control point through crypto solutions
  - The reality: a separable question
  - Finkhäuser: "control over the algorithms employed is typically centralized"
- Abe Chen: If users do not have independent identity for communication through a system, they cannot communicate directly → users rely upon a focal facility serving the coordination functions → network operation becomes centralized

“Secrets & Lies
Digital Security in a Networked World” by Schneier

I have written this book partly to correct a mistake.

Seven years ago I wrote another book: *Applied Cryptography*. In it I described a mathematical utopia: algorithms that would keep your deepest secrets safe for millennia, protocols that could perform the most fantastical electronic interactions-unregulated gambling, undetectable authentication, anonymous cash-safely and securely. In my vision cryptography was the great technological equalizer; anyone with a cheap (and getting cheaper every year) computer could have the same security as the largest government.... I went so far as to write: “It is insufficient to protect ourselves with laws; we need to protect ourselves with mathematics.”

It’s just not true. Cryptography can’t do any of that.

It’s not that cryptography has gotten weaker since 1994, or that the things I described in that book are no longer true; it’s that cryptography doesn’t exist in a vacuum.

Cryptography is a branch of mathematics... Security, palpable security that you or I might find useful in our lives, involves people: things people know, relationships between people, people and how they relate to machines...

Steering the Internet away from further consolidation, and towards decentralizing control: how?

Huitema: Need to "commoditize" a number of platform components -- naming and discovery, introduction, etc

- focus on a few applications. The good platforms components almost always come after the application.
- Developing platforms before developing applications seems rational, but it almost never works for software.
- So maybe identify a couple of applications first

Summary

1. **Measurements**
   - Continueing to measure and document the level of centralization, its effects, new developments
   - Assessing the degree of “decentralization” in proposed systems (web3, blockchain)
2. **Improving understanding**
   - System issues vs. control issues
   - Root causes and potential mitigation strategies: e.g., universal user identities
3. **Overcoming decentralization**
   - Platforms and applications
   - What is the best, realistic role that DINRG can play?
     - Forum for discussing current research and key technologies
     - Incubator for projects (platforms, applications)