

Default Safe: Realizing the Potential of Decentralized Networks

Brien Colwell, URnetwork

Background

Launched URnetwork in 2025 as a decentralized overlay network to deliver IP privacy and global content access.

Running with zero known issues for users and participants. Learned key principles with 180k users around the world - 100 countries, 3000 cities.

Potential of decentralized systems

Compute and network devices are ubiquitous. 1.5B+ new smartphones/year, 8B+ new consumer electronics/year [1,2]

The ability to tap into excess resources can create new infrastructure that benefits from scale - e.g. privacy, compute, storage, sensor - with order-of-magnitude lower operating costs than alternative architectures

Transparency and give-to-get are strengths of decentralized models, making the infrastructure more trustworthy and accessible

1. <https://www.statista.com/outlook/cmo/consumer-electronics/telephony/smartphones/worldwide>
2. <https://www.statista.com/markets/418/topic/485/consumer-electronics>

Major problems with decentralized systems

Safety is actually two problems:

- Risks to Users
- Risks to Participants

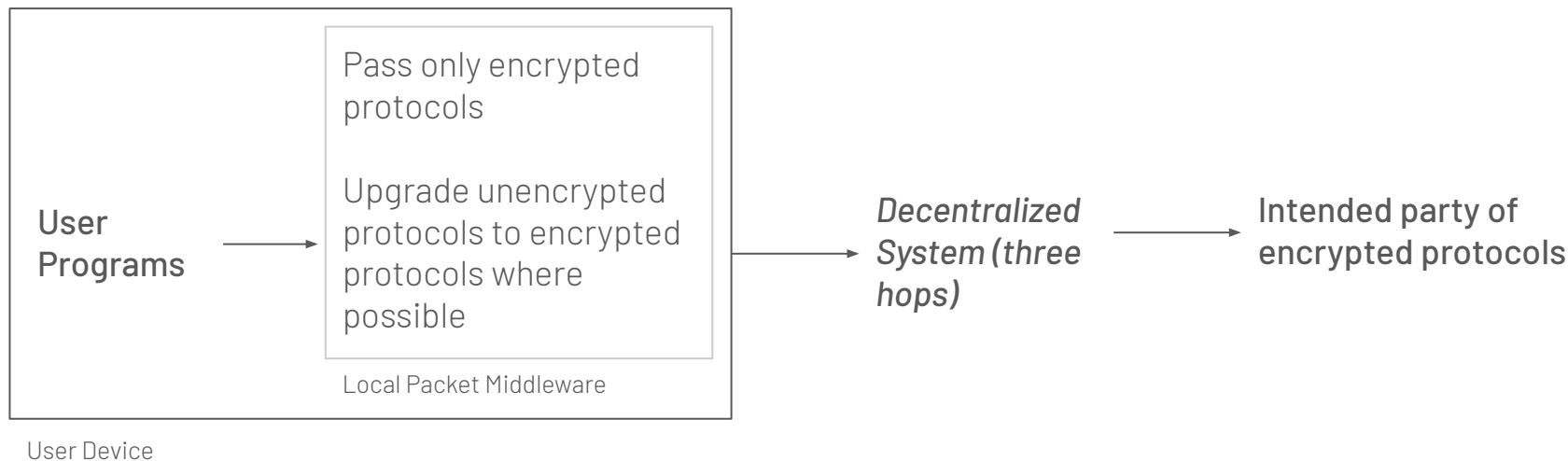
Reliability

URnetwork uses a few key principles to create a safe, scalable, and ethical product. These principles can help inform any decentralized system.

Safety: Risks to users

A key principle is to allow only encrypted data into the system. If data cannot be encrypted through the decentralized system, the system might not be a good candidate for decentralization.

For example in a network, a protocol packet flow looks like the following.

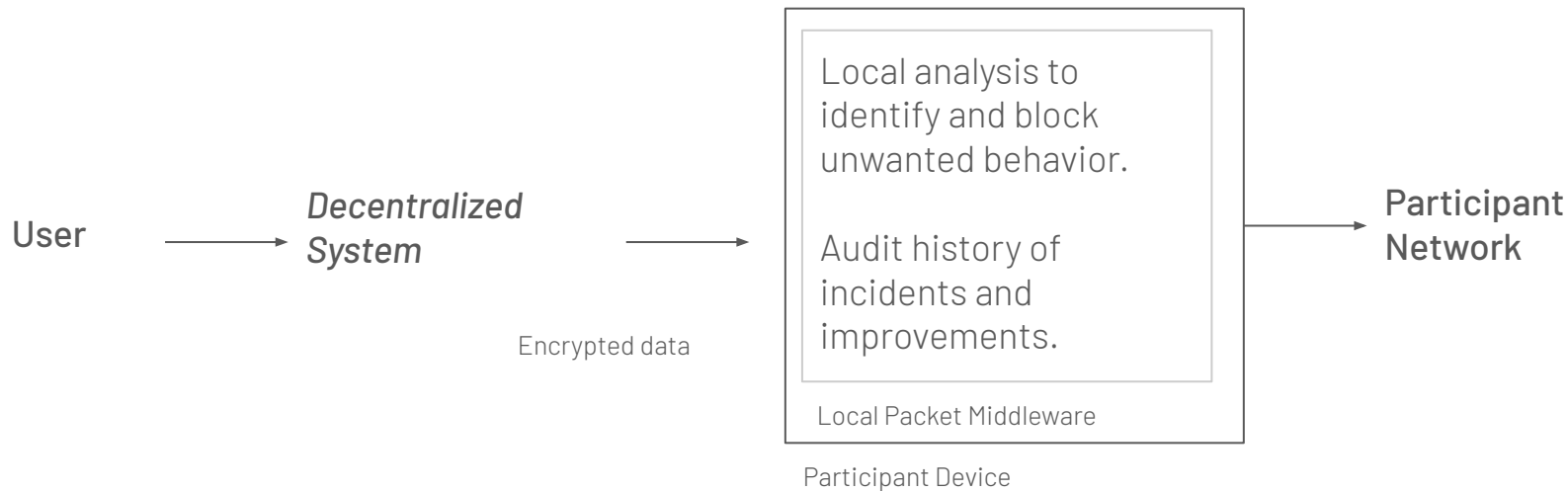


Safety: Risks to participants

Participants have a duty of care to respond and fix issues, and possibly limit access to users from some locations. For example in the US, Computer Fraud and Abuse, DMCA, and Iran export.

A key principle is to run a security program on the participant side to identify and block unwanted behavior. Improvements to the program are in public to prove responsiveness. Key approaches are blocking ports (e.g. reserved ports), IPs (known IP lists), and protocols (e.g. P2P).

Safety: Risks to participants



1. https://github.com/urnetwork/connect/blob/main/ip_security.go

Safety: Open research problems

Protocol detection aligned with intent is a major issue. For example most P2P traffic is fine, but file sharing is an issue. It would generally help to have robust BitTorrent protocol detection.

Reliability: Ground in real infrastructure

A key principle is that participants on real infrastructure align with the interests of users. Virtual infrastructure is easy to alias, fast to change, and hard to measure decentralization, reliability, and capacity.

Online IP classification can help. Use MMDB to classify IP addresses ephemeraly so that user information does not have to be saved or leave the service.

Virtual networks - ARINDB [1]

Virtual networks and compute - Various IP meta data providers

1. <https://github.com/urnetwork/arindb>

Principles for safe decentralized systems

- Only encrypted data in
- Auditable local security for participants with access controls
- Limit virtual infrastructure

Q&A

Brien Colwell <brien@ur.io>

<https://discord.gg/urnetwork>

@xcolwell (Signal, TG, Discord)