IRTF
Decentralized Internet Infrastructure
Proposed Research Group
Scope Discussion
Interim Meeting at NDSS-2018

Dirk Kutscher  Melinda Shore

2018-02-17, San Diego, CA, USA
Decentralized Internet Infrastructure

- Investigate open research issues in decentralizing infrastructure services
  - Trust management, identity management
  - Name resolution, resource/asset ownership management, resource discovery

- Focus: infrastructure services that can benefit from decentralization
  - Or that are difficult to realize in local, potentially connectivity-constrained networks

- Objectives
  - Investigate use cases and requirements with respect to implementing them in a distributed manner
  - Discuss and assess solutions with a focus on Internet level deployment issues such as scalability, performance, and security
  - Develop and document technical solutions and best practices
  - Develop tools and metrics to identify scaling issues and to identify missing components
  - Identify future work items for the IETF
Background (IRTF)

- Had a few meetings at previous IETF meetings
- “Distributed Internet Infrastructure”
  - [https://trac.ietf.org/trac/irtf/wiki/blockchain-federation](https://trac.ietf.org/trac/irtf/wiki/blockchain-federation)
- Topics
  - Applying distributed ledger (blockchain et al.) to Internet technologies
  - Distributed protocol id/name registry
  - Infrastructure services for IoT -- avoiding centralized services etc.
  - Data and service federation in future telco networks
- Summary so far
  - There is interest -- seems like a good topic for the IRTF
  - Most interesting: Internet infrastructure services based on distributed ledger tech
Motivation

- Internet was designed as a distributed, decentralized system
  - Intra- and inter-domain routing, DNS
- Dominant deployment model for applications and some infrastructure services evolved to become more centralized and hierarchical
  - Sometimes/often due to business models that rely on centralized accounting and administration
- New: evolution of use cases (e.g., certain IoT deployments) that cannot work well in centralized deployment scenarios
- Evolution of decentralized technologies
  - Leverage new cryptographic infrastructures like DNSSEC
  - Using novel, cryptographically-based distributed consensus mechanisms, such as a number of different ledger technologies.
Evolution of Distributed Ledger Tech

- Has given rise to the development of & experiments with decentralized communication and infrastructure systems
  - Name resolution (Namecoin, Ethereum Name Service)
  - Identity management (OneName)
  - Distributed storage (IPFS, MaidSafe)
  - Distributed applications, or DApps (Blockstack)
  - IP address allocation and delegation and many more

- Systems differ with respect to
  - Problems solved
  - Specific technologies that they apply
  - Consensus algorithms that are employed
  - Incentives that are built into the system

- Goal: investigate these systems from an Internet technologies perspective
  - connect the domain expertise in the IRTF and IETF with the distributed systems and decentralized ledgers community
Research Challenges and Activities for DINRG

● Scalability
  ○ What are the problems that prevent decentralized infrastructure services from achieving global scale?
● Trust management in decentralized communication settings
● Privacy and targeted, verifiable disclosure
● Applicability of distributed ledger and related technologies to different use cases and environments
● Consensus algorithms for specific scenarios
  ○ With a focus on Internet infrastructure services
● Ability of constrained nodes to benefit from elements of a consensus item that they cannot process or store as a complete set
● Distributed Trust and Delegated Computing
● Economic drivers and roadblocks for decentralizing network infrastructure
● Identification of common requirements and properties of selected technologies
● Design and implementation of one or more general-purpose infrastructure systems
● Deployment and operation of one or more actual implementations
Use Case Areas Discussed So Far

- Decentralizing Internet infrastructure
  - Address allocation
  - Registries
  - Name resolution
- Decentralizing web infrastructure
  - Decentralizing communication platforms, data sharing
- Decentralizing trust management
  - For example, decentralizing OAuth, enabling cloudless authorization, on-boarding etc.
- Decentralized resource management
  - For example, wireless interference management
- IoT network infrastructure (constrained/disconnected environments)
  - Finding data, services
  - Nano-payments

Observation
Not all of these address/requires Internet-scale scalability
Comments, Questions, Discussion?