Towards an Interoperability Architecture for Blockchain Autonomous Systems

Thomas Hardjono (MIT)
Alexander Lipton (MIT, Sila)

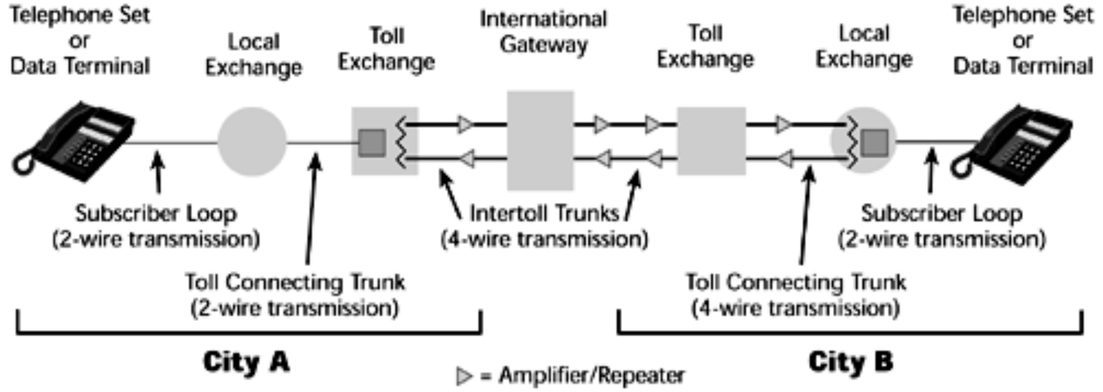
MIT Connection Science & Engineering
Massachusetts Institute of Technology

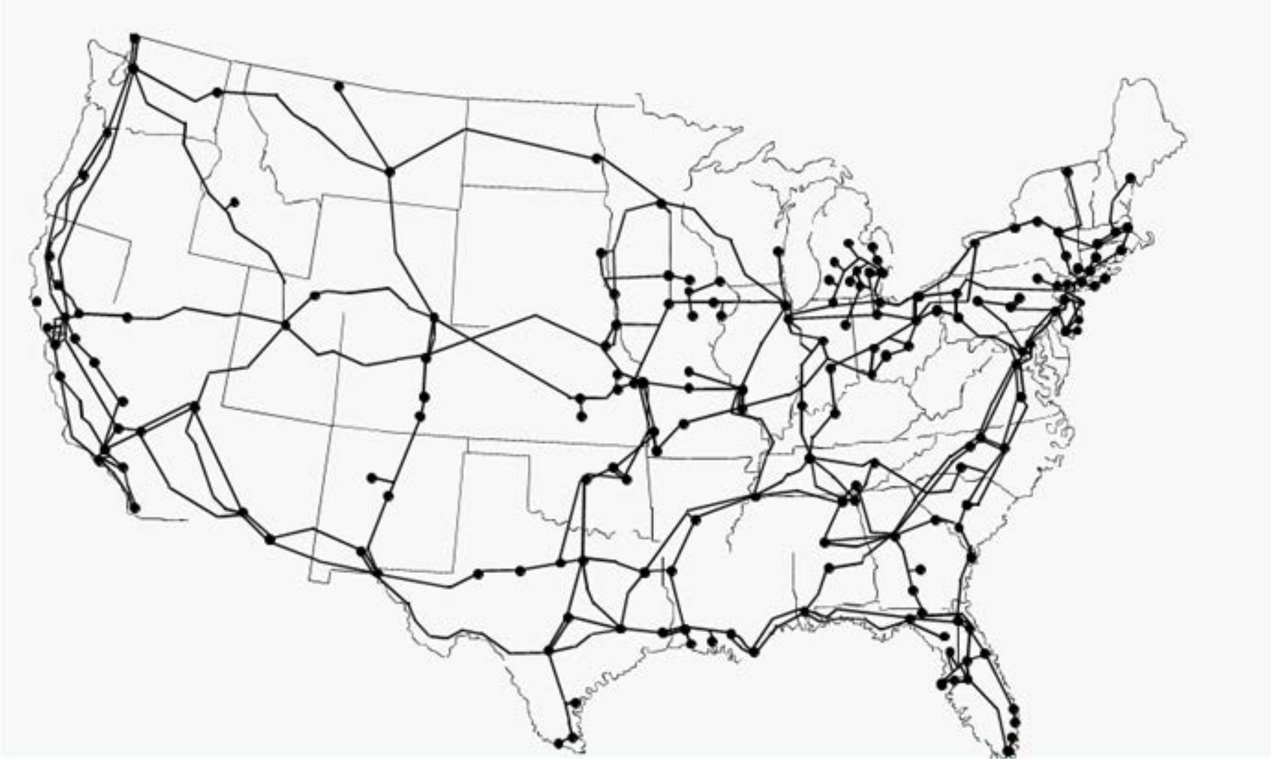
hardjono@mit.edu

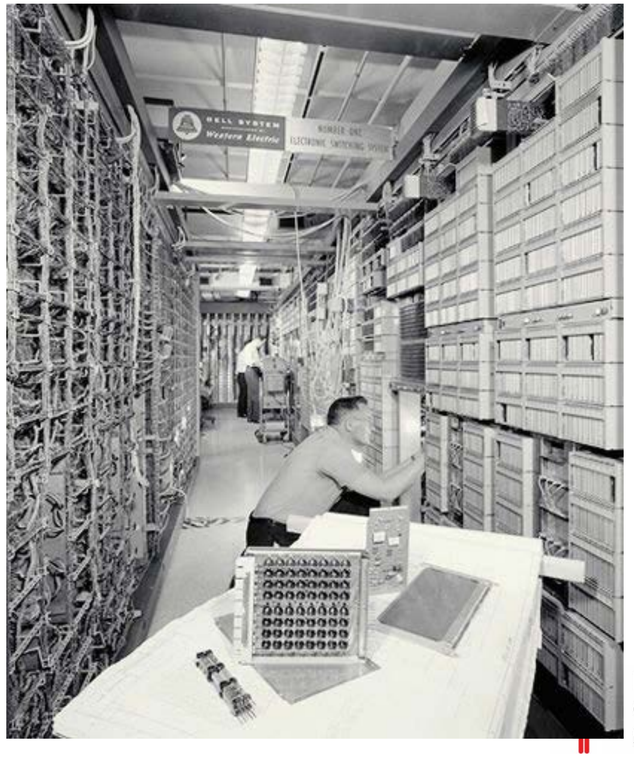
ITU DLT Meeting
5 August 2020

MIT Connection Science

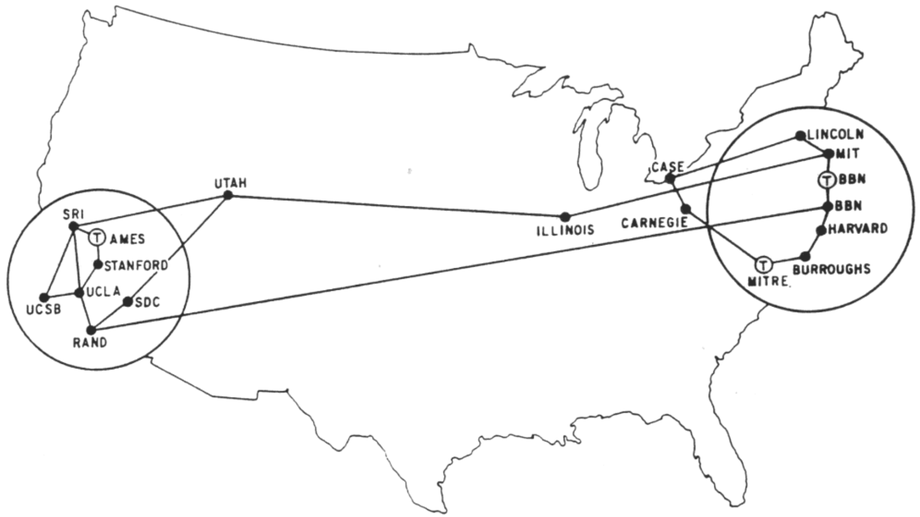
The Telephone Network: Fragility



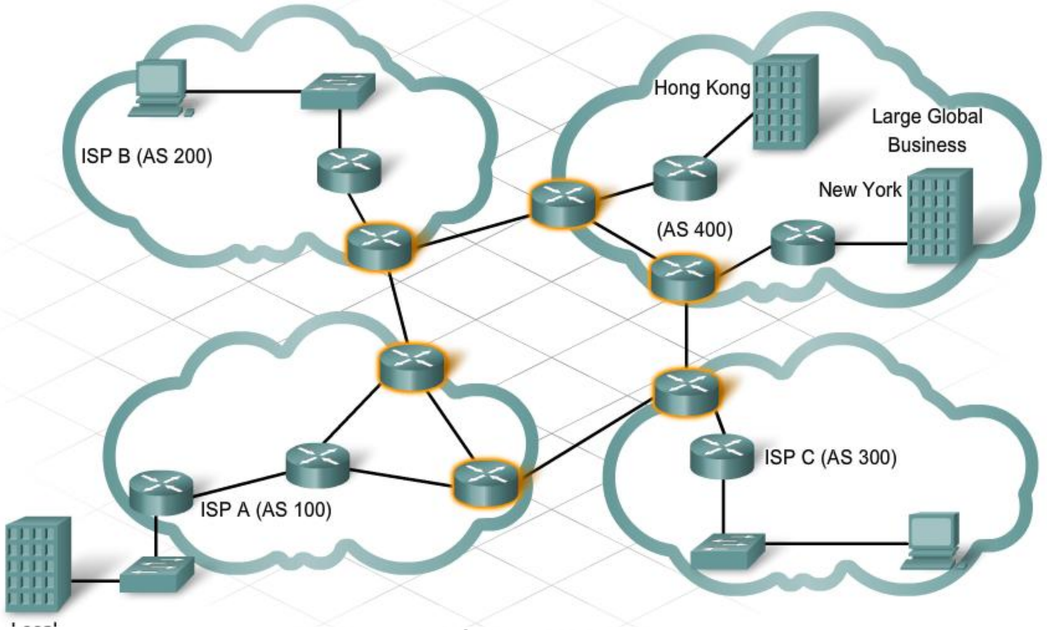




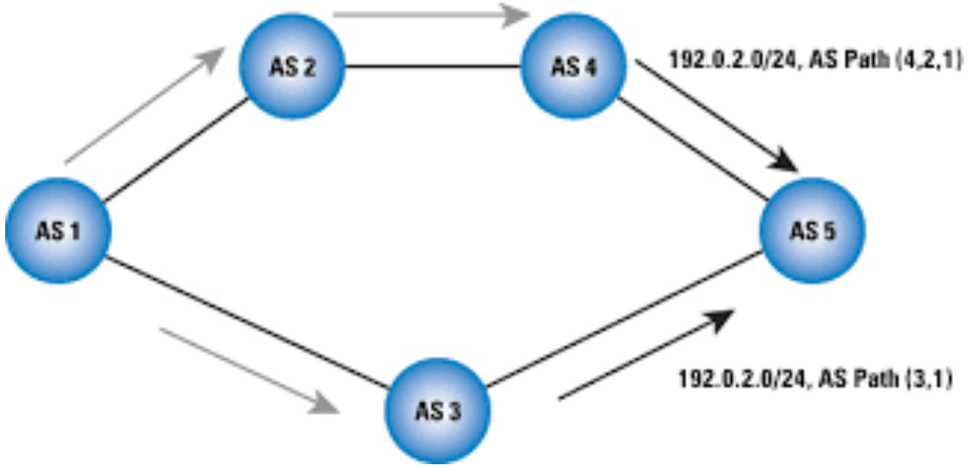
The Internet: Datagram, multiple routes

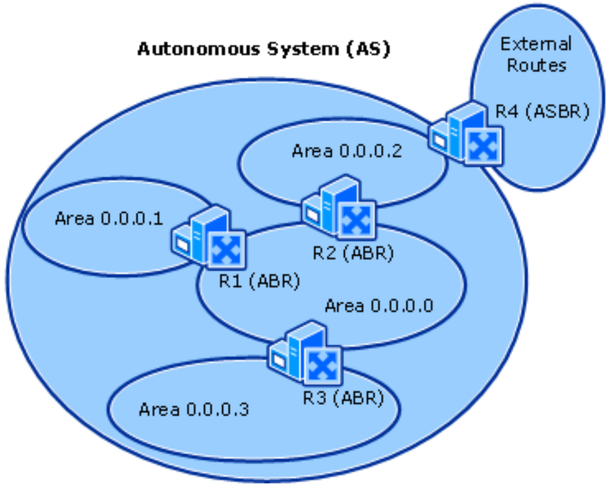


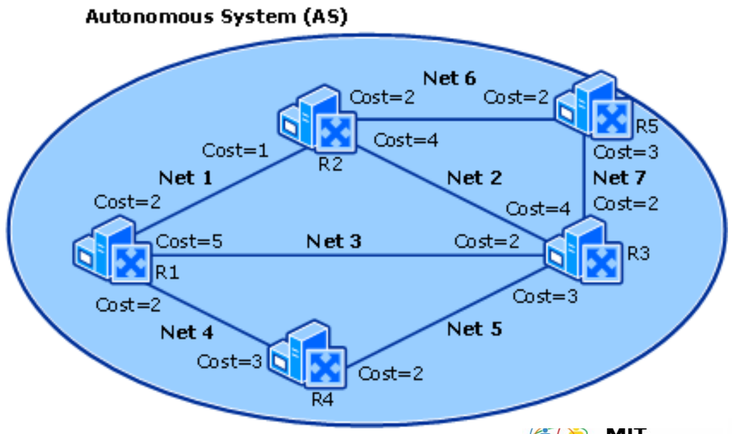
MAP 4 September 1971



Network Using RIP Routing







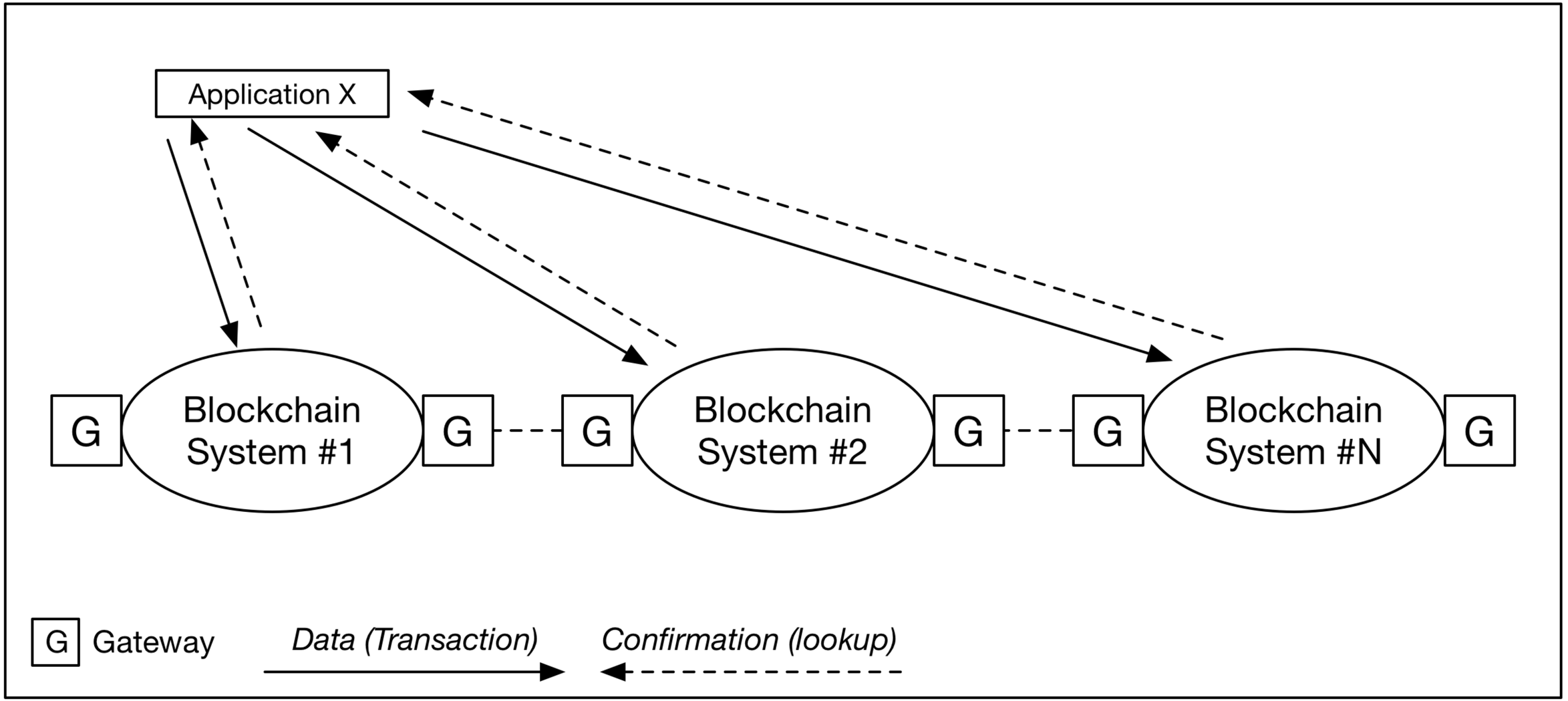
MIT Connection Science

Internet Architecture: Fundamental Goals

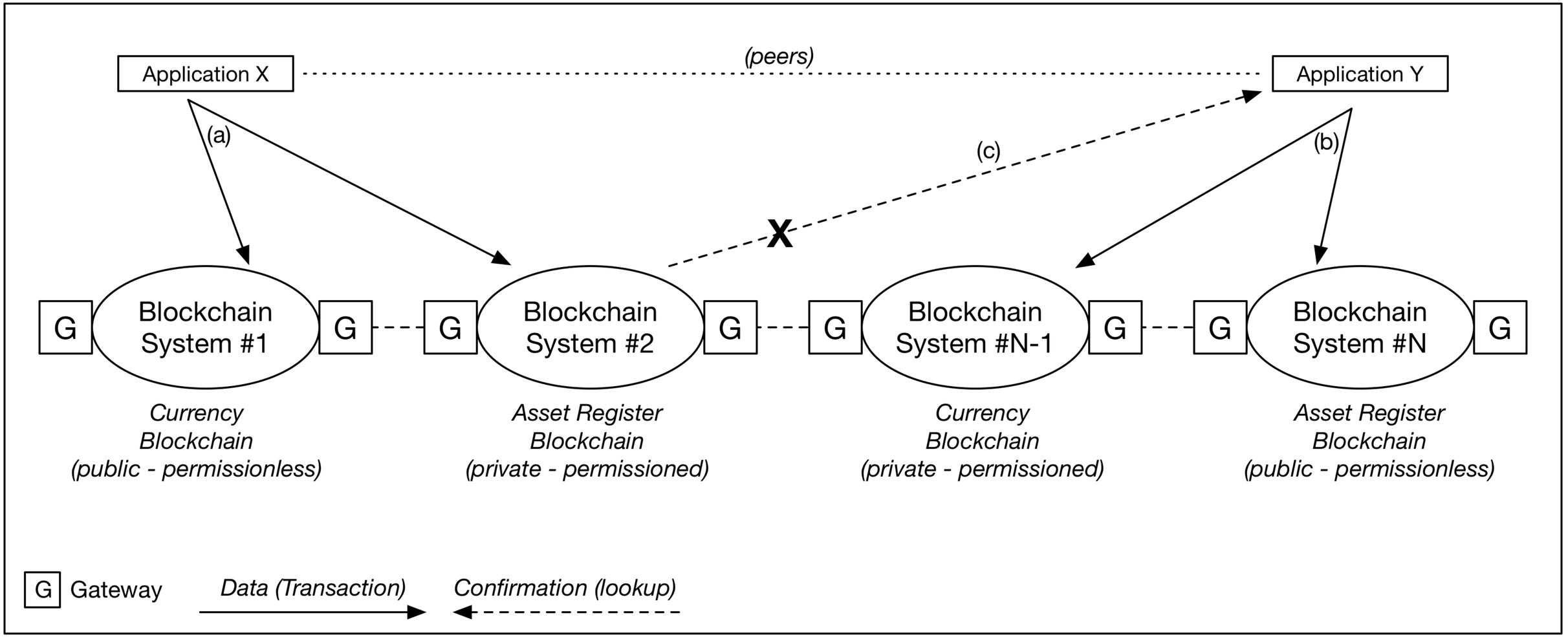
- *Survivability*: Internet communications must continue despite loss of networks or gateways
- *Variety of service types*: support multiple types of communications service
- *Variety of networks*: accommodate a variety of networks

David Clark, The Design Philosophy of the DARPA Internet Protocols, August 1988.

Blockchain Reliability Issues



Cross-Chain Limitations



Blockchain Survivability Issues

- Infrastructure level concerted attacks (e.g. DDOS attacks)
- Sophisticated manipulation of consensus algorithms
- Weaponization of legitimate applications (e.g. DAO, CryptoKitties, Flash trades, etc.)
- Asset lock-in

Lessons Learned from Internet Architecture

- Interoperability fundamental to survivability
- View each blockchain as a bounded and independent system – Autonomous Systems paradigm
- Standardize basic transaction format
- Alternative business models (e.g. subscription)
- Peering agreements (SLA)

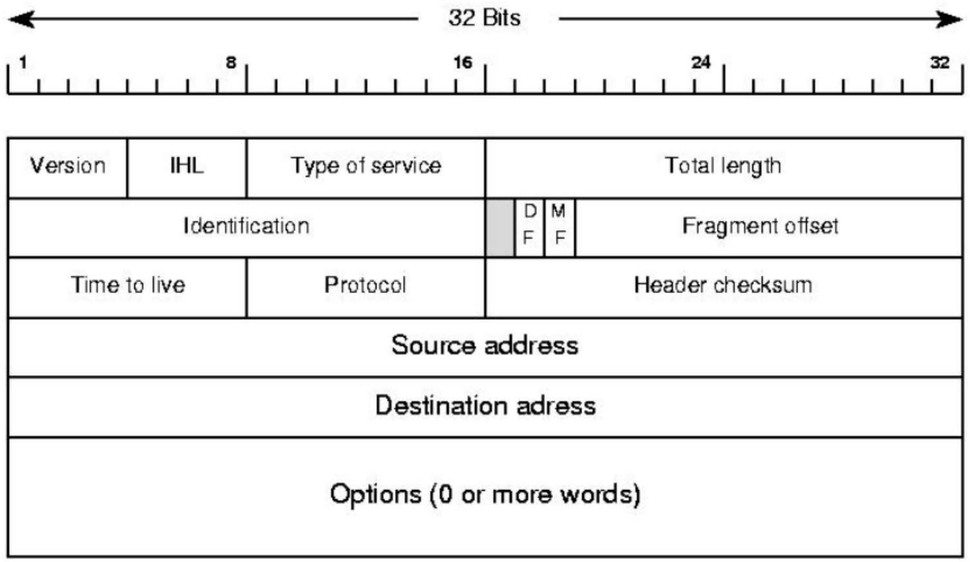
Standardization of Transaction ``Packet”

- Blockchain system identifier
- Sender address (public-key)
- Receiver address (public-key)
- Operation (op-code)
- Pointer to asset (hash)
- Timestamp
- Signature

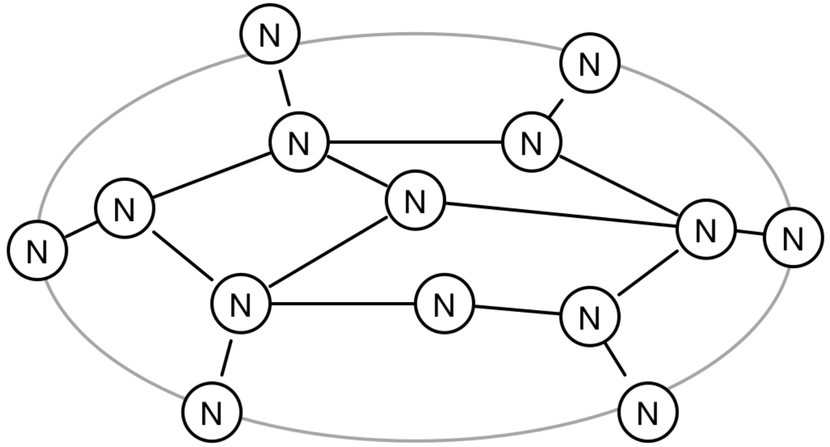
A Protocol for Packet Network Intercommunication

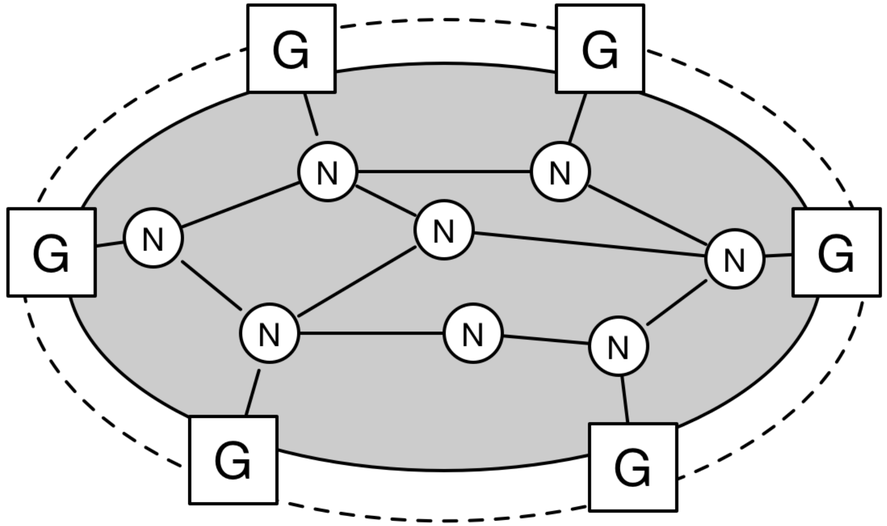
VINTON G. CERF AND ROBERT E. KAHN,
MEMBER, IEEE

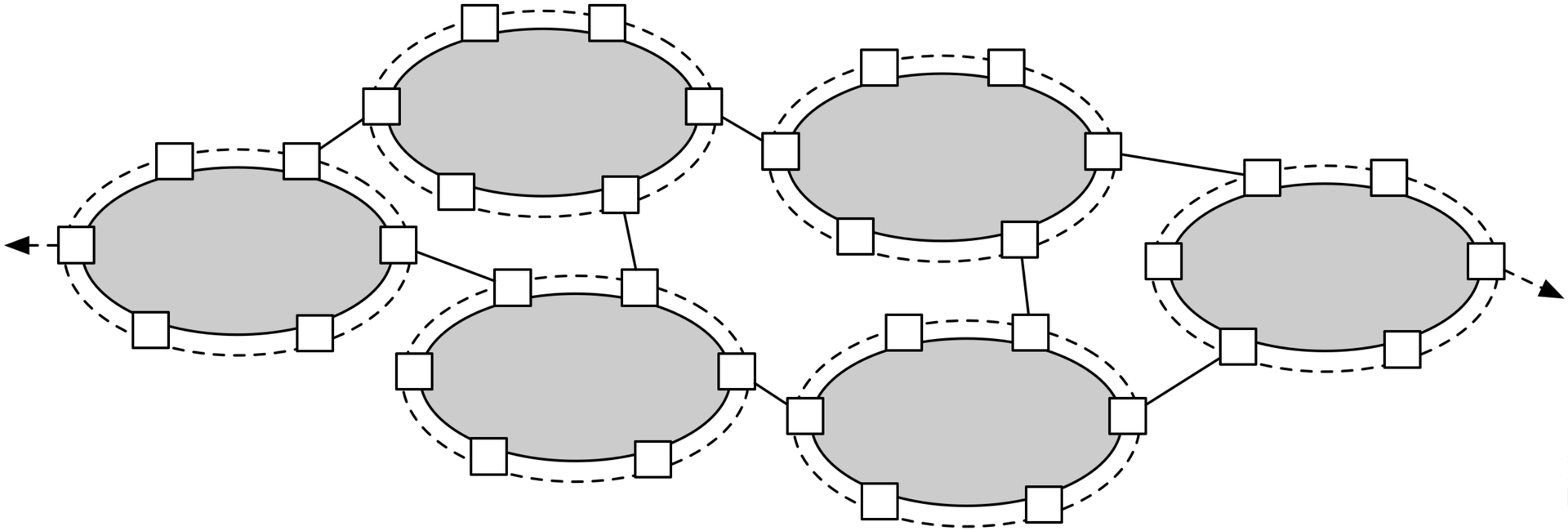
IEEE Trans on Comms, Vol Com-22, No 5 May 1974



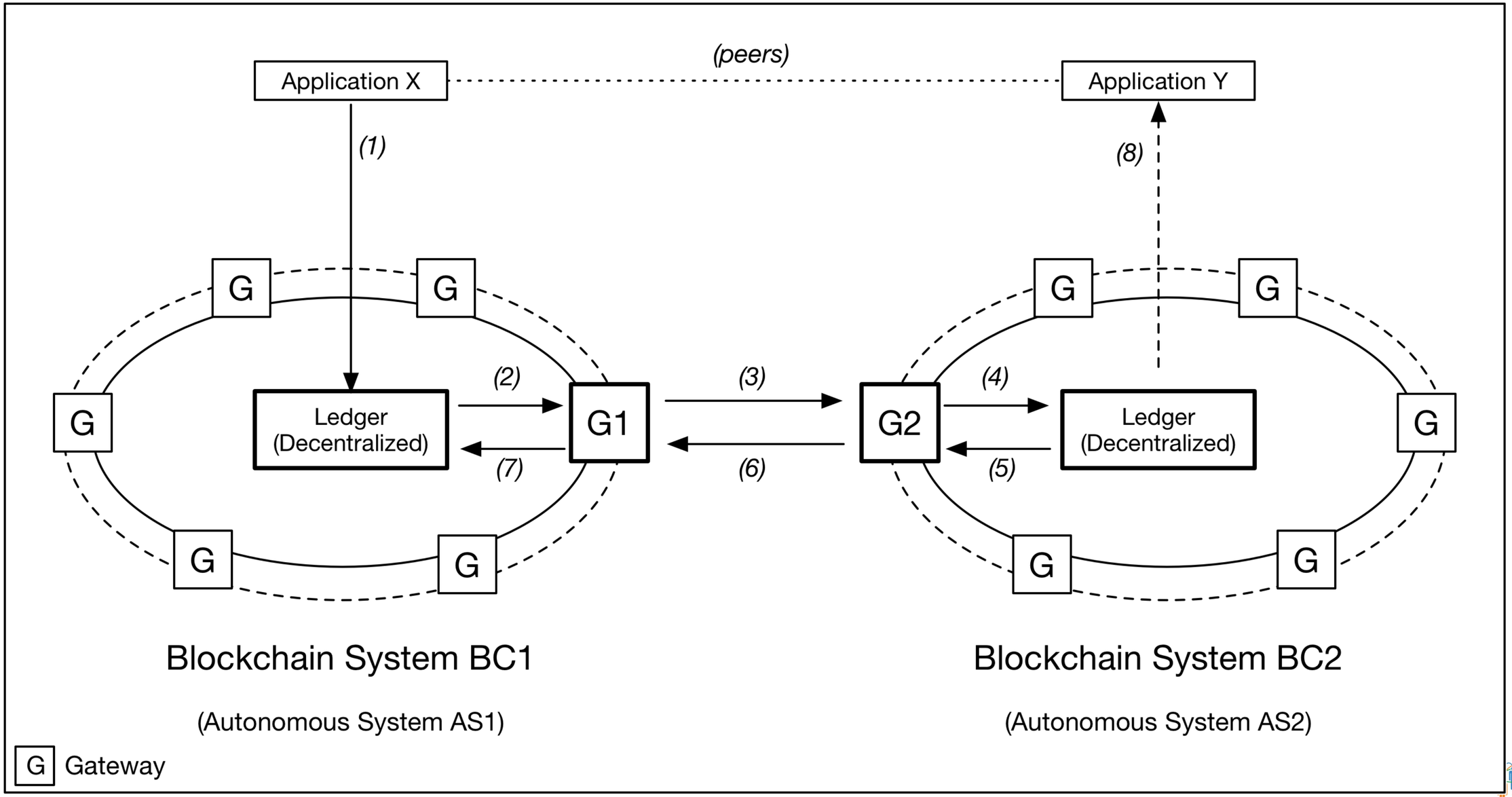
Peering between blockchains







Peering Model



Conclusion

- Designing for survivability is designing for scale
- Interoperability is crucial for survivability
- Blockchain systems are autonomous systems
- Nodes/clients must be identifiable and authenticable
- Peering Model (Contracts)

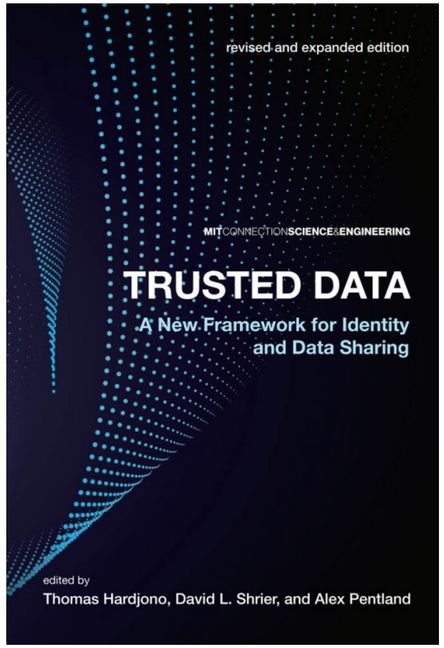
Thank You

Thomas Hardjono, Ph.D.
CTO
Connection Science & Engineering

Massachusetts Institute of Technology
77 Massachusetts Avenue, Building E18
Cambridge, Massachusetts 02139

Email hardjono@mit.edu
Phone +1 781-729-9559
Twitter @FindThomas

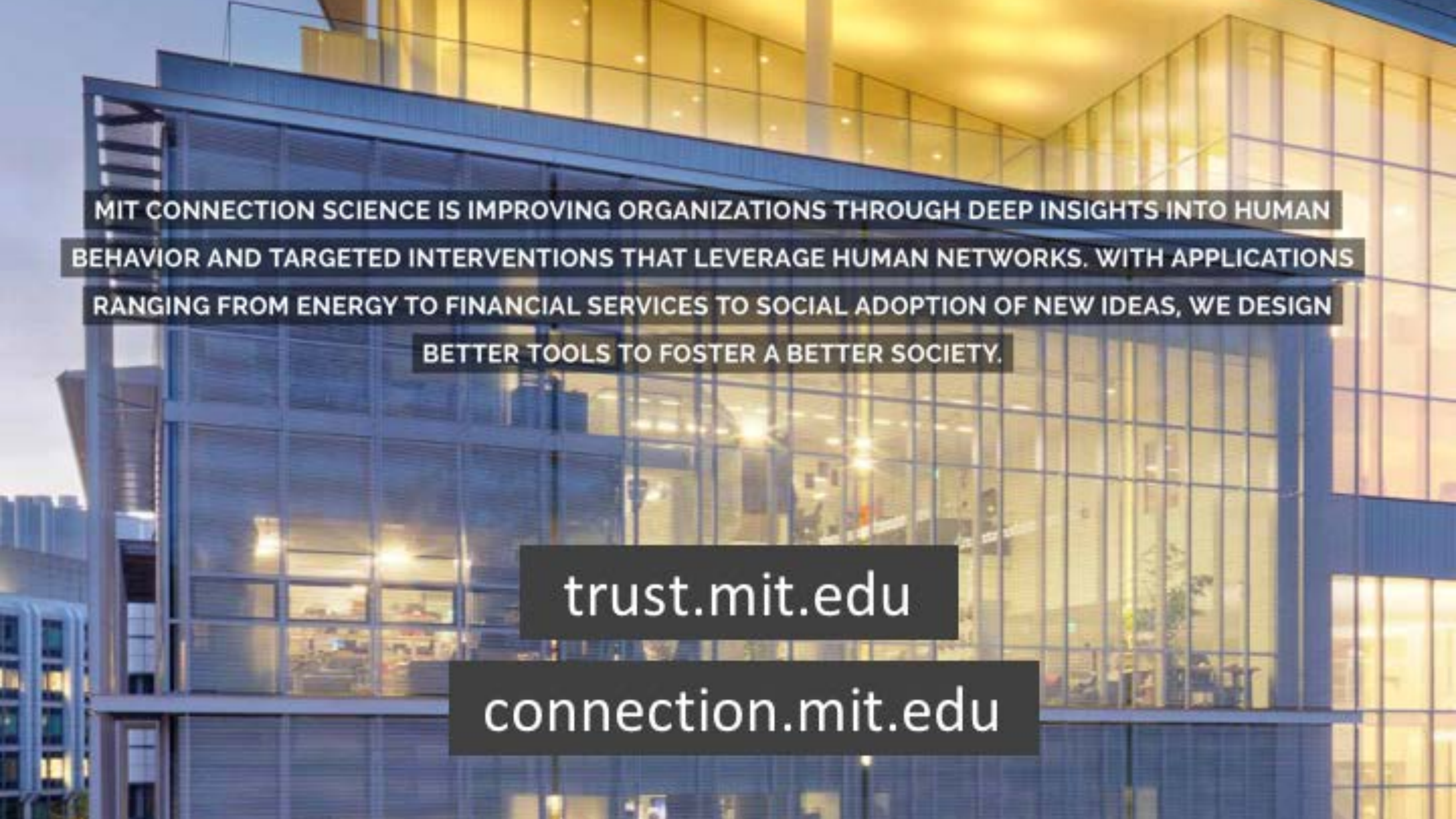
connection.mit.edu



"Design Philosophy for Interoperable Blockchain Systems", *IEEE Transactions on Eng Mgmt* (2019)
https://arxiv.org/pdf/1805.05934

Building the New Economy (MIT Press, 2020)
https://wip.mitpress.mit.edu/new-economy

MIT Connection Science


MIT CONNECTION SCIENCE IS IMPROVING ORGANIZATIONS THROUGH DEEP INSIGHTS INTO HUMAN BEHAVIOR AND TARGETED INTERVENTIONS THAT LEVERAGE HUMAN NETWORKS. WITH APPLICATIONS RANGING FROM ENERGY TO FINANCIAL SERVICES TO SOCIAL ADOPTION OF NEW IDEAS, WE DESIGN BETTER TOOLS TO FOSTER A BETTER SOCIETY.
trust.mit.edu
connection.mit.edu