Blockchain Interoperability and Survivability

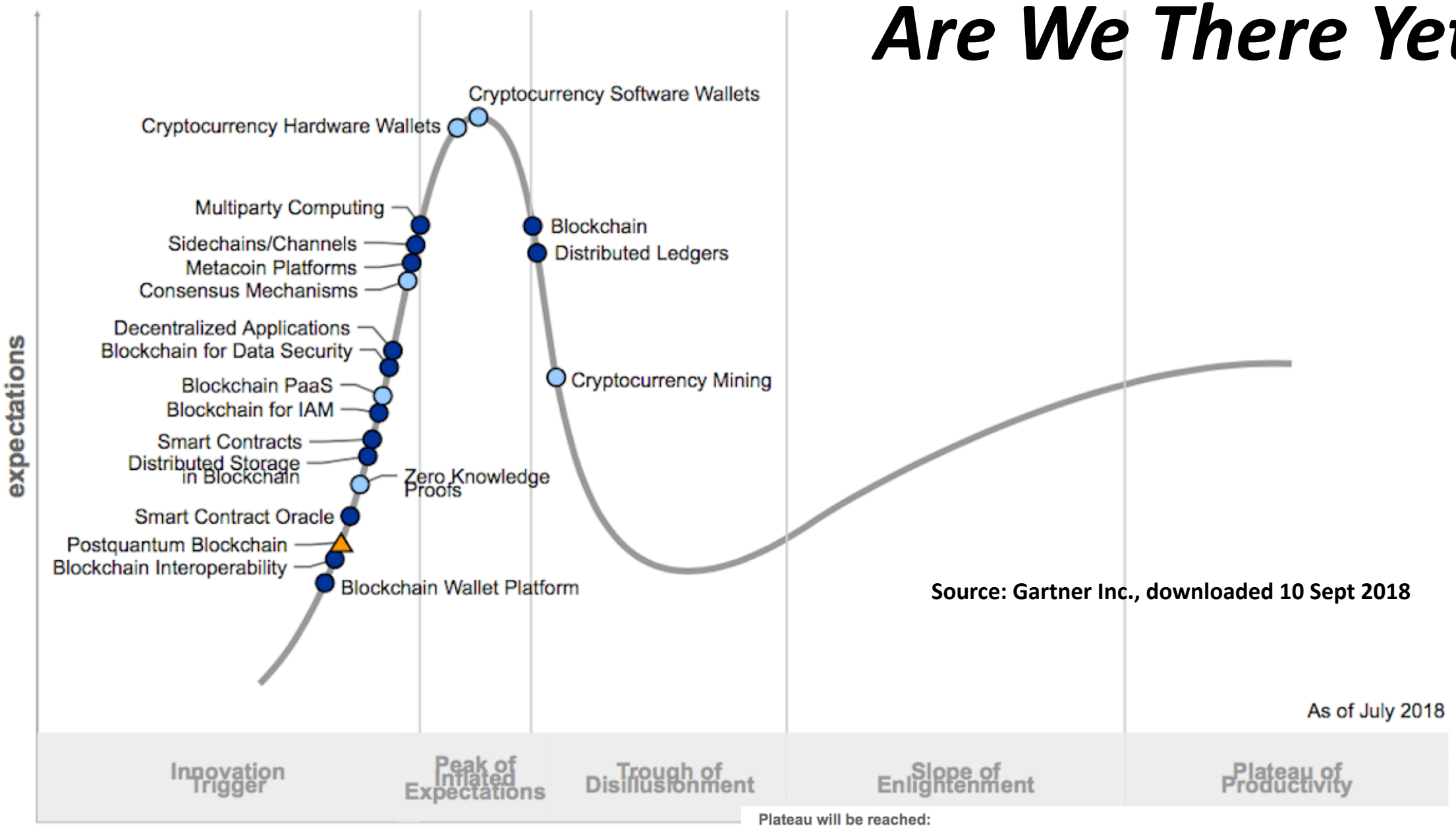
Thomas Hardjono

MIT Connection Science

2018 IEEE Global Blockchain Summit

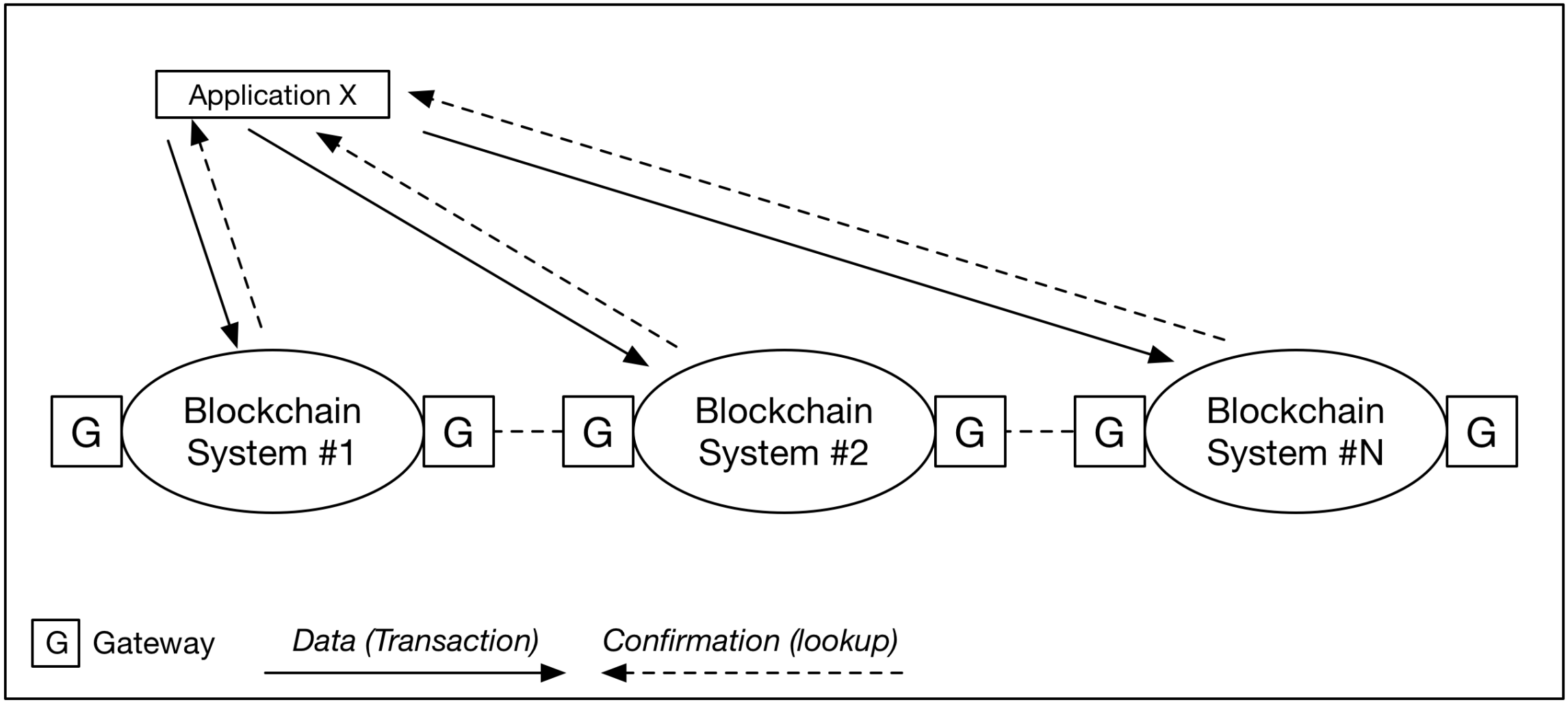
17-19 September 2018

Are We There Yet…

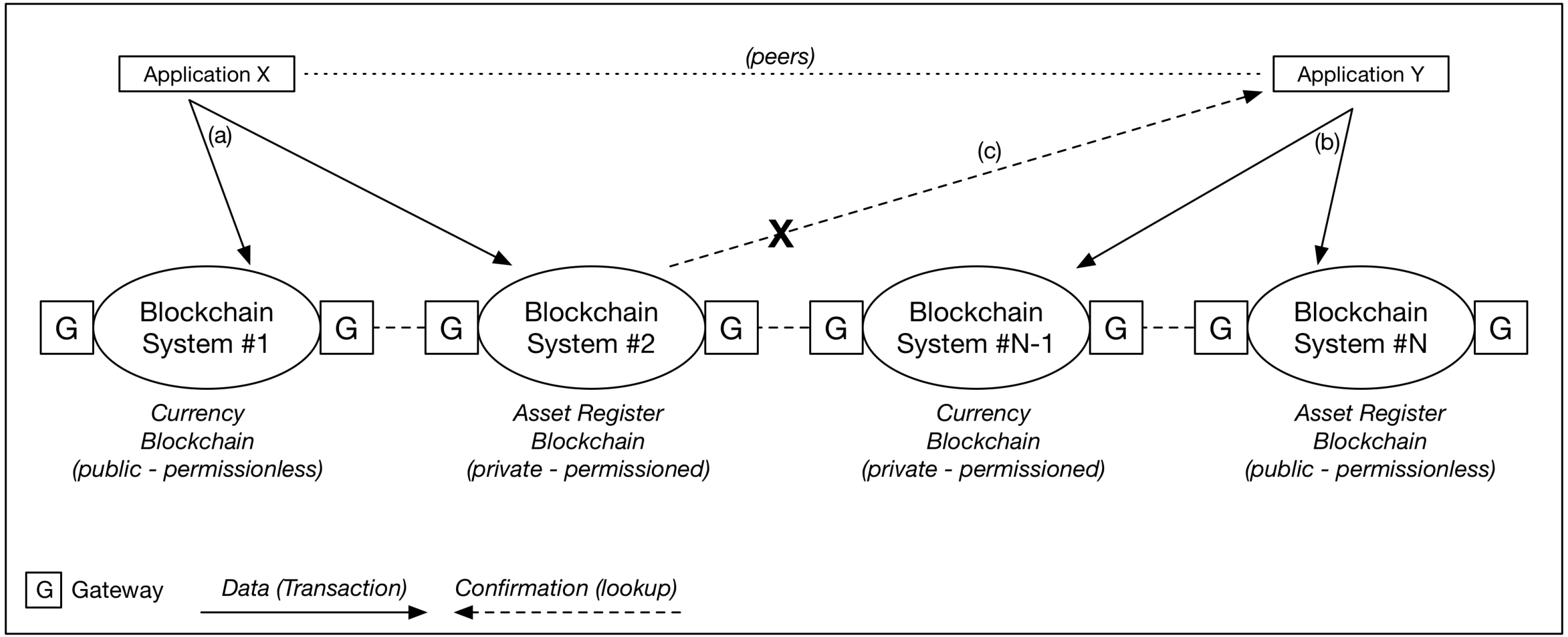


Source: Gartner Inc., downloaded 10 Sept 2018

Reliability Challenges



Cross-Permissions Challenges



Can a Blockchain System Survive…

Infrastructure level concerted attacks

Sophisticated manipulation of consensus algorithms

Weaponization of legitimate applications (e.g. DAO, CryptoKitties)

Viruses targeted to specific mining software

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.

Internet Architecture: Lessons Learned

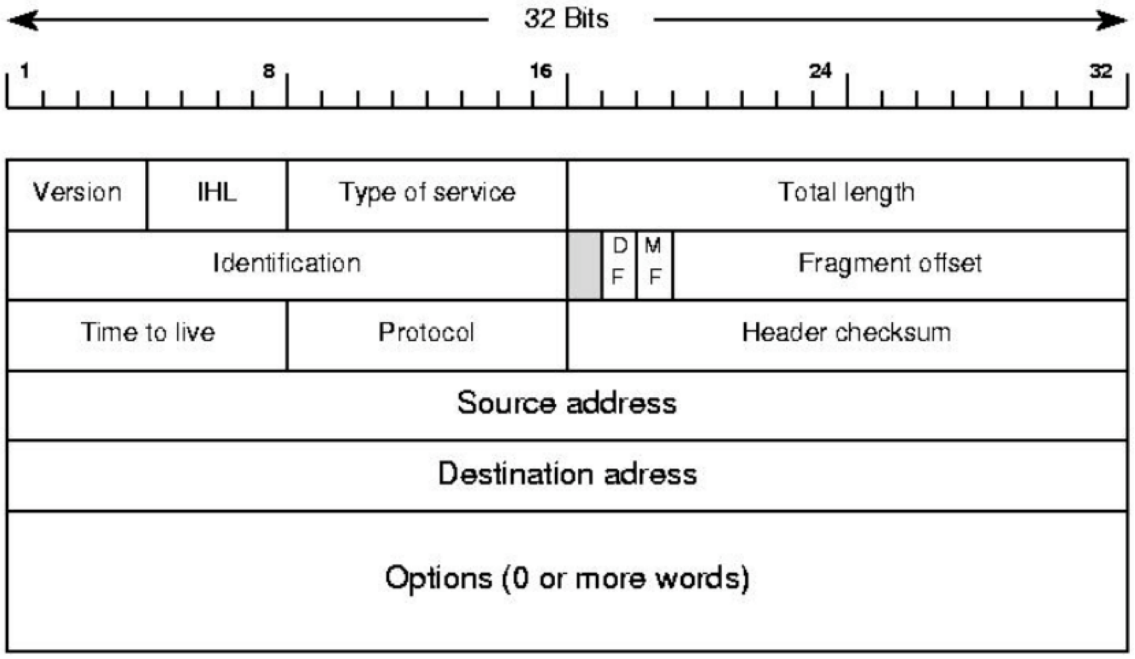
Interoperability across networks as fundamental to survivability of the whole

Each network as a bounded and independent system – *Autonomous Systems paradigm*

The *IP Datagram* as the lowest common denominator

Peering of ISPs as core business incentive

IP Datagram: Lowest Common Denominator



What is the blockchain equivalent of the IP Datagram?

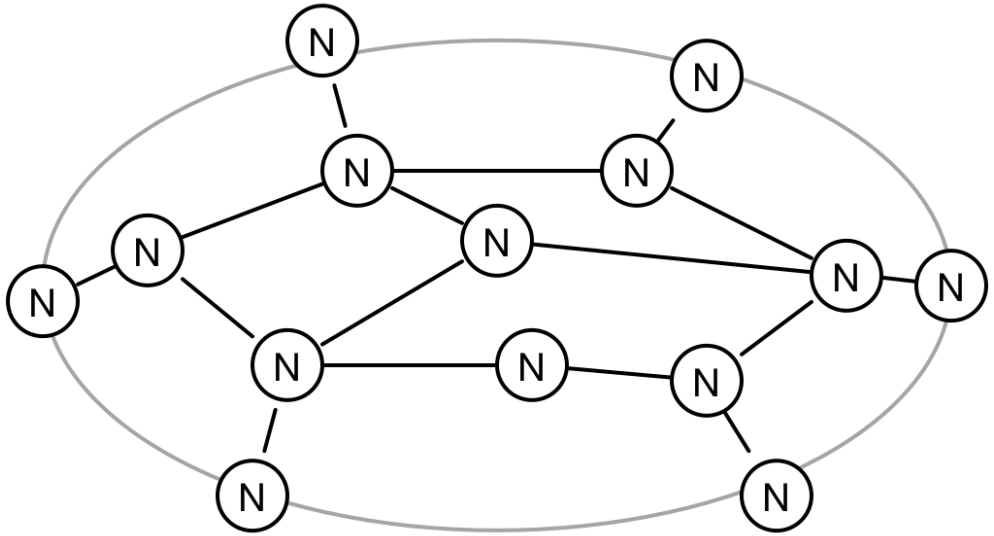
What are the common primitive operation(s)

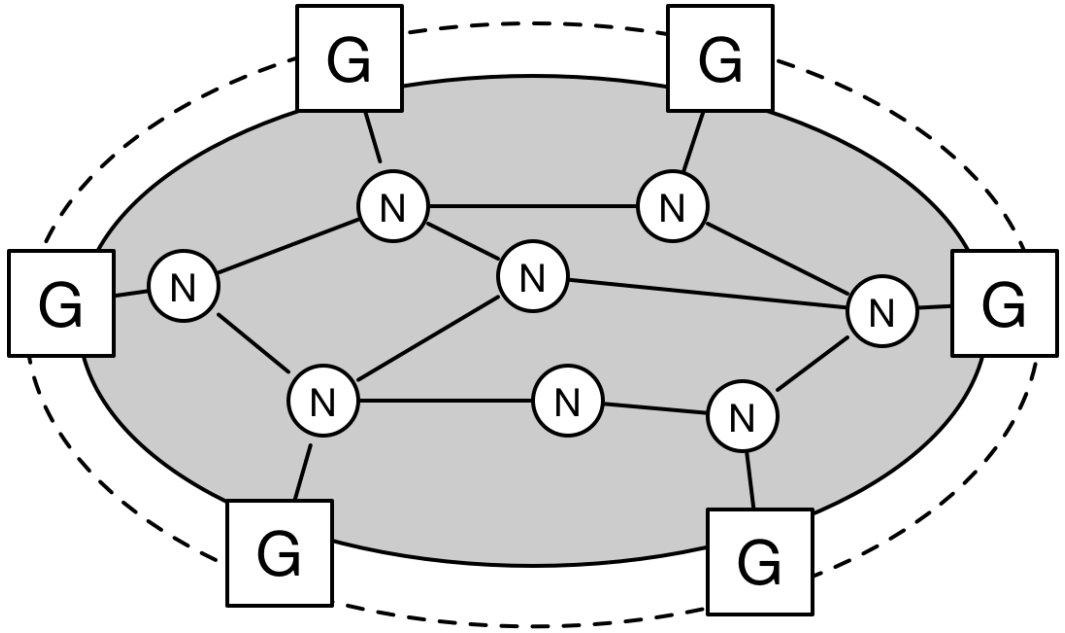
A Protocol for Packet Network Intercommunication

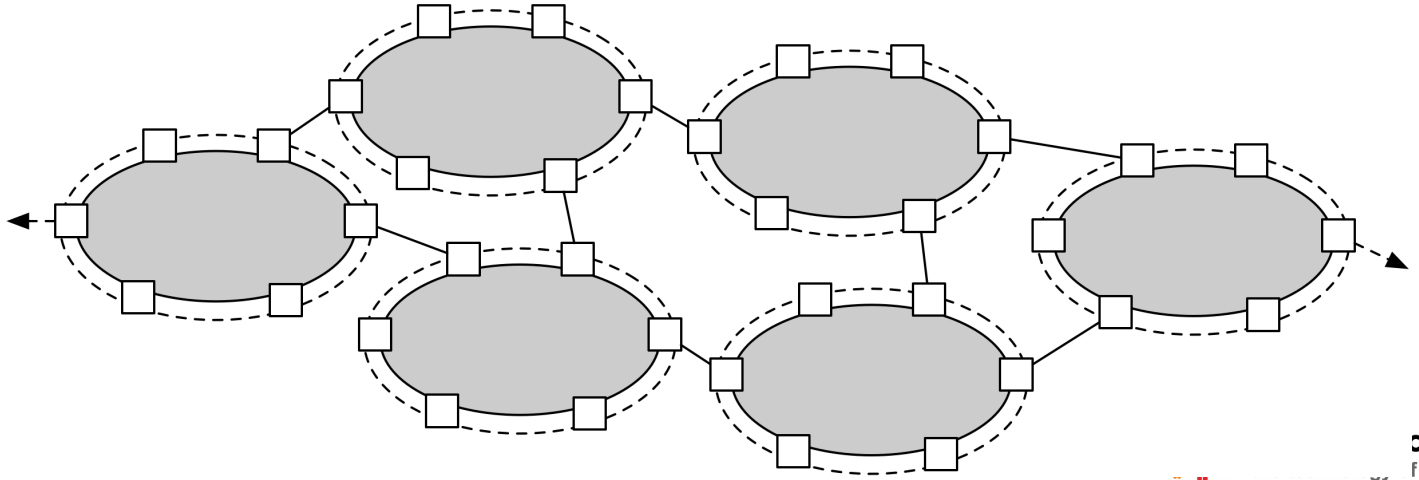
VINTON G. CERF AND ROBERT E. KAHN,
MEMBER, IEEE

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

Autonomous Systems & Gateways







Definition: An Interoperable Architecture

An interoperable blockchain architecture is a composition of distinguishable blockchain systems,

each representing a unique distributed data ledger,

where *atomic transaction execution may span multiple blockchain systems*,

and where data recorded in one blockchain is *reachable, verifiable and referenceable* by another possibly foreign transaction

in a *semantically compatible* manner.

Some Open Challenges

How to define the *perimeter* of a blockchain autonomous system

What is the standard for the atomic *transaction unit* (minimal assumption)

How to interoperate across two or more *permissioned* systems

How to identity & authenticate nodes

What is the business model for peering

Key Take-Aways

Designing for survivability is designing for scale

Interoperability is crucial for survivability

Blockchain systems *are* autonomous systems

Blockchain infrastructure components must be identifiable and authenticable

trust.mit.edu

connection.mit.edu