A Proposal to Improve MANRS Global Secure Internet Routing Policy Management Using Blockchain Technology

Version 1.1
June 6, 2020

William Favre Slater, III
slater@billslater.com
williamslater@gmail.com
Chicago, IL
United States of America

Table of Contents

Executive Summary

This blog will explain the highlights and the importance of what we learned in the ISOC MANRS Global Secure Routing Course, and then propose how Blockchain technologies can be used to further enhance the MANRS processes that have been established to provide secure Internet Routing.

What We Learned in the ISOC MANRS Global Secure Routing Course

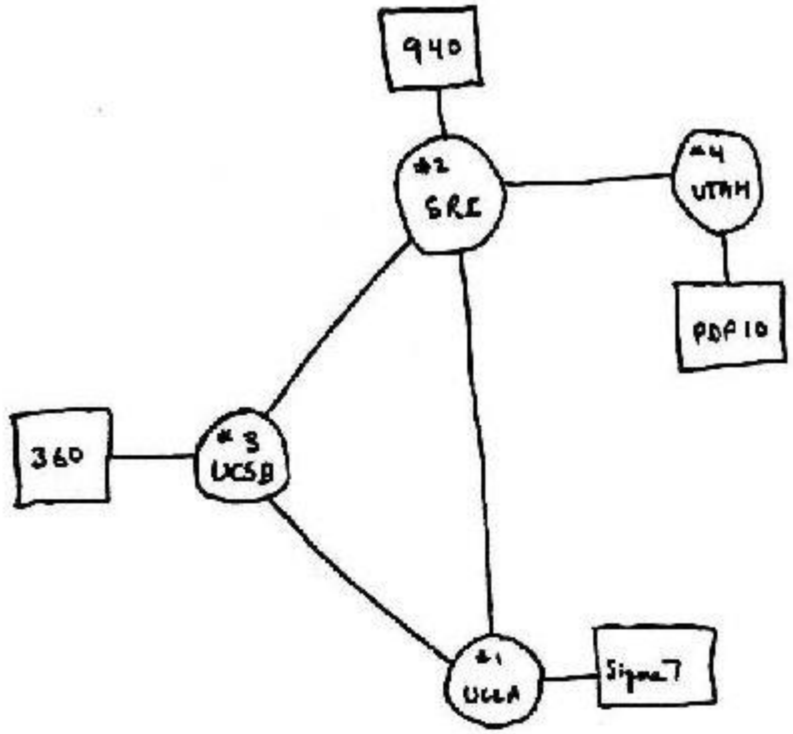
This is the agenda for the ISOC MANRS Global Secure Routing Course:

- Routing Protocols with emphasis on BGP
- BPG and Global Routing Security
- Incidents Caused by Routing Errors
- What MANRS Is, How It Works and Why It Is Important
- Internet Routing Registries (IRR) and the Role They Play in Secure Internet Routing Infrastructure
- Internet Routing Registries (IRRs)
- Resource Public Key Infrastructure (RPK)
- PeeringDB
- Creation of a Network Policy
- Global Validation
- How Network Policies Work From a Practical Perspective
- Open Source Tools Used to Develop and Register Network Policies
- Filtering Techniques and Why We Use Them
- Anti-Spoofing Techniques and Why We Use Them
- Coordination and Techniques, Including Registration, Roles, and Responsibilities

Introduction – Beginning at the Beginning

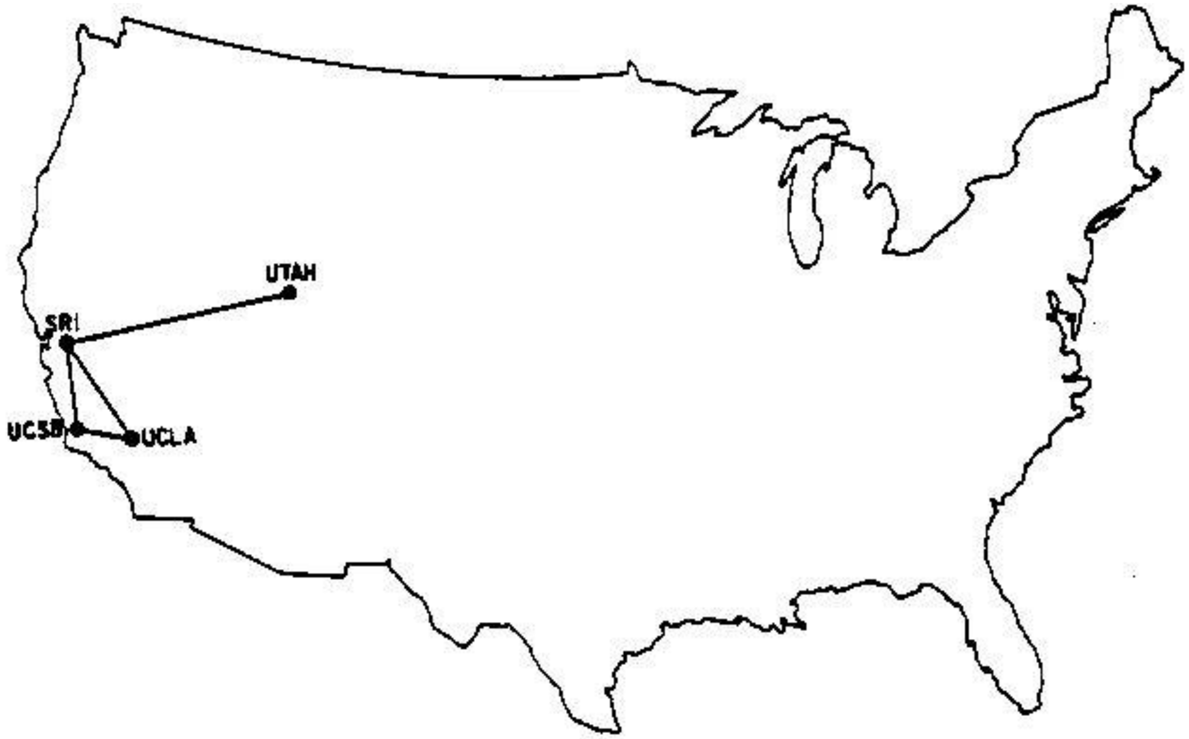
The Internet began in 1969 as the ARPANET Project successfully used electronic communications to transmit messages between four centralized computers. The pictures below show the original ARPANET.

From Computer Desktop Encyclopedia
Reproduced with permission.
© 2000 The Computer Museum History Center

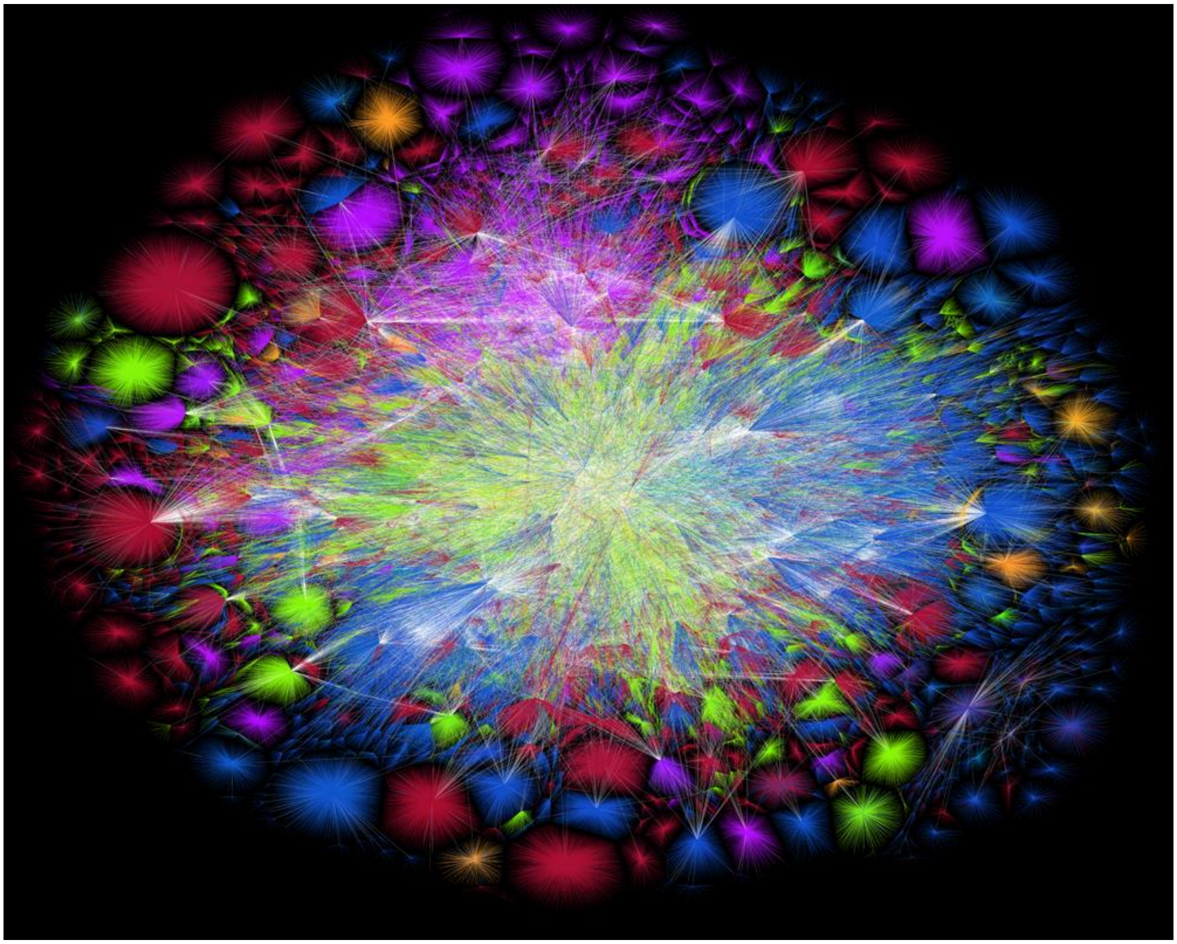


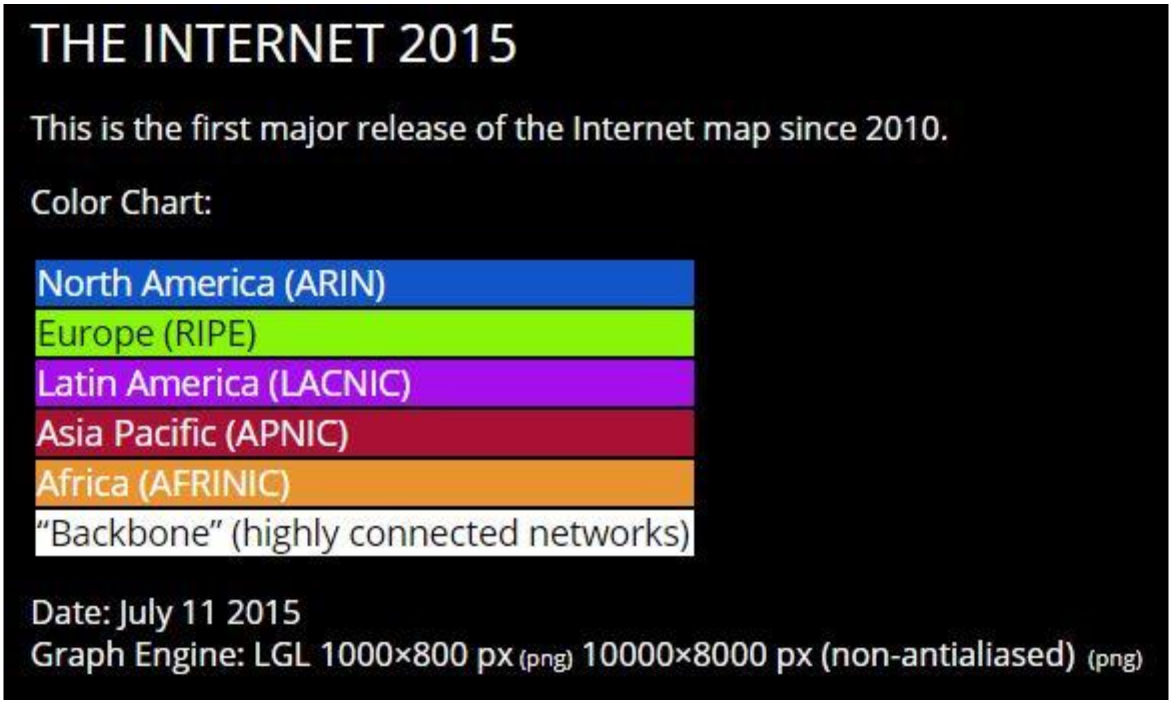
Humble Beginnings

Scrawled on this paper in 1969 were the first four nodes of the ARPANET. Little did they realize these four nodes would grow to millions. (Image courtesy of The Computer History Museum, www.computerhistory.org)



The big color picture below from opte.org is a visualization of the Internet as it was in 2015.





THE INTERNET 2015

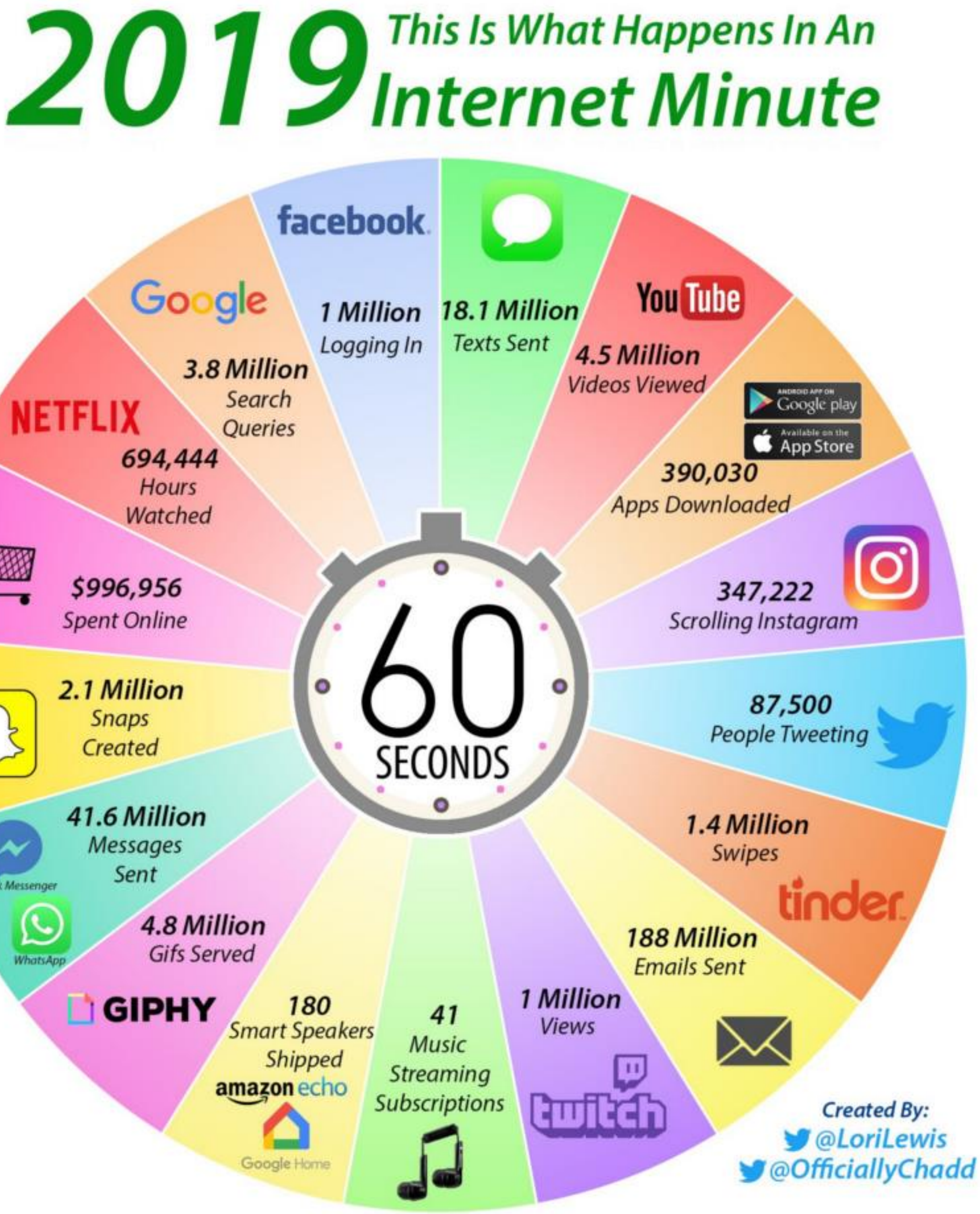
This is the first major release of the Internet map since 2010.

Color Chart:

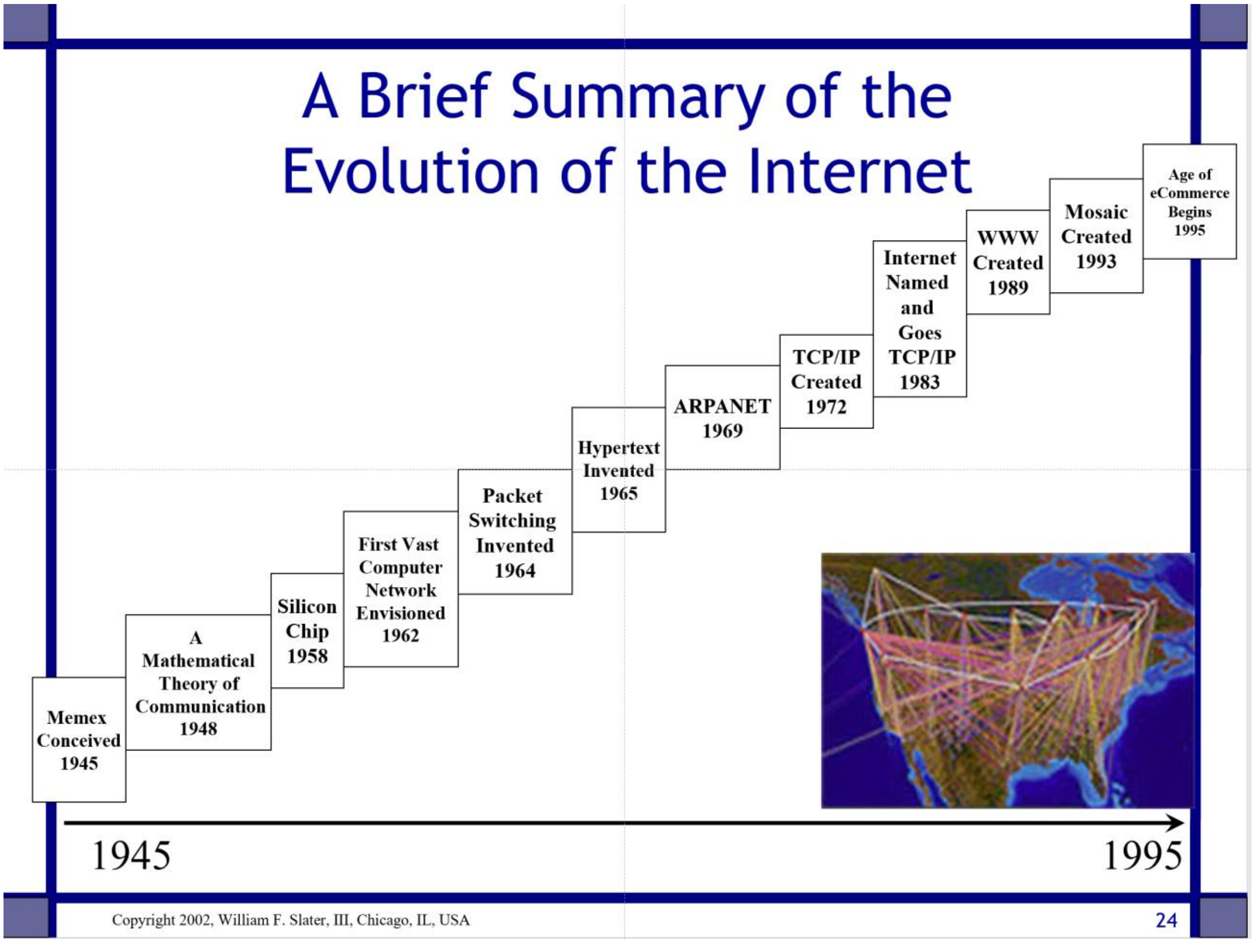
- 🟦 North America (ARIN)
- 🟩 Europe (RIPE)
- 🟪 Latin America (LACNIC)
- 🟥 Asia Pacific (APNIC)
- 🟧 Africa (AFRINIC)
- ⬜ “Backbone” (highly connected networks)

Date: July 11 2015
Graph Engine: LGL 1000×800 px (png) 10000×8000 px (non-antialiased) (png)

The diagram below shows how people typically interacted with the Internet every 60 seconds in 2019.



The diagram below shows a high-level summary of how the Internet evolved from a conceptual idea to the time when it became an environment for e-commerce in the 1990s.



A Brief Summary of the Evolution of the Internet

Memex Conceived 1945

A Mathematical Theory of Communication 1948

Silicon Chip 1958

First Vast Computer Network Envisioned 1962

Packet Switching Invented 1964

Hypertext Invented 1965

ARPANET 1969

TCP/IP Created 1972

Internet Named and Goes TCP/IP 1983

WWW Created 1989

Mosaic Created 1993

Age of eCommerce Begins 1995

1945

1995

Copyright 2002, William F. Slater, III, Chicago, IL, USA

24

The rapid growth of e-commerce as well as the "dot-com" explosion from 1996 - 2000 made the Internet go "business critical" somewhere between 1997 to 1998. This not only meant that most organizations were adopting an online presence of their physical self, but that they were beginning to expect having Internet access on a 24 x 7 basis, including websites, e-mail, and e-commerce transactions. As these expectations continued, a transformation to a 'Digital Economy" occurred, and downtime was not considered to be acceptable and in fact, it was considered to be a detriment to the viability of any organization that could not be up on the Internet on a 24 x 7 basis.

The Internet of the 21st Century has evolved into an environment that is heavily dependent on connected Cloud Data Centers, Cloud-based applications, and mobile applications. This requires a responsive, reliable, low-latency, network of networks to support these applications. Then with the onset of the global CoronaVirus Pandemic in March 2020, with social distancing requirements and the need for precautionary measures to slow the spread of this highly contagious virus, organizations started ordering their employees and contractors to work from home, in other words, to Telework as a standard business practice. Whereas employees had formerly been used to going to work and connecting to their employer's Internet connection, now they are relying on their home Internet Service Provider (ISP) to get out to the Internet to get their organization's work accomplished. The Cloud and mbile applications are still very much in the picture, but the reality and ubiquity of telework for foreseeable has led ISPs to have to work with major Internet carriers to add new networking equipment and reconfigure their connections to optimize these new, unexpected Internet traffic patters and usage loads.

It should be noted here that one of the biggest reasons for the successful evolution of the Internet as an environment / resource that most people in the civilized world depend on, is free, well-written standards and the organized framework for testing, evaluating, and publishing these standards. These are the RFCs (Request for Comments). The RFCs may be considered as the evolving "Constitution" of the Internet, and they are usually developed and approved by members of the Internet Engineering Task Force. The entire body of RFCs are located in these locations for public viewing:

www.rfc-editor.org

www.ietf.org

www.faqs.org

www.rfc-editor.org/rfcxx00.html (where xx represents the number of the RFC)

The diagram before shows the types of RFCs and how they get published.

Types of RFCs

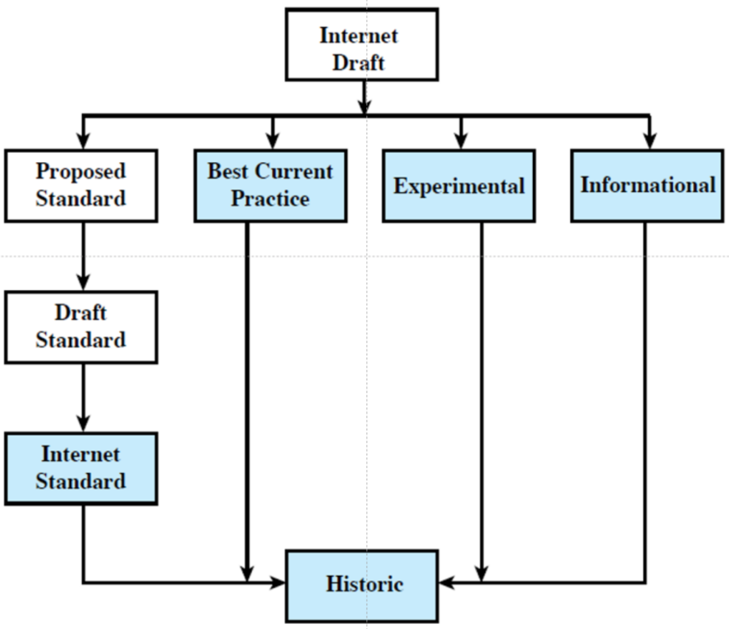
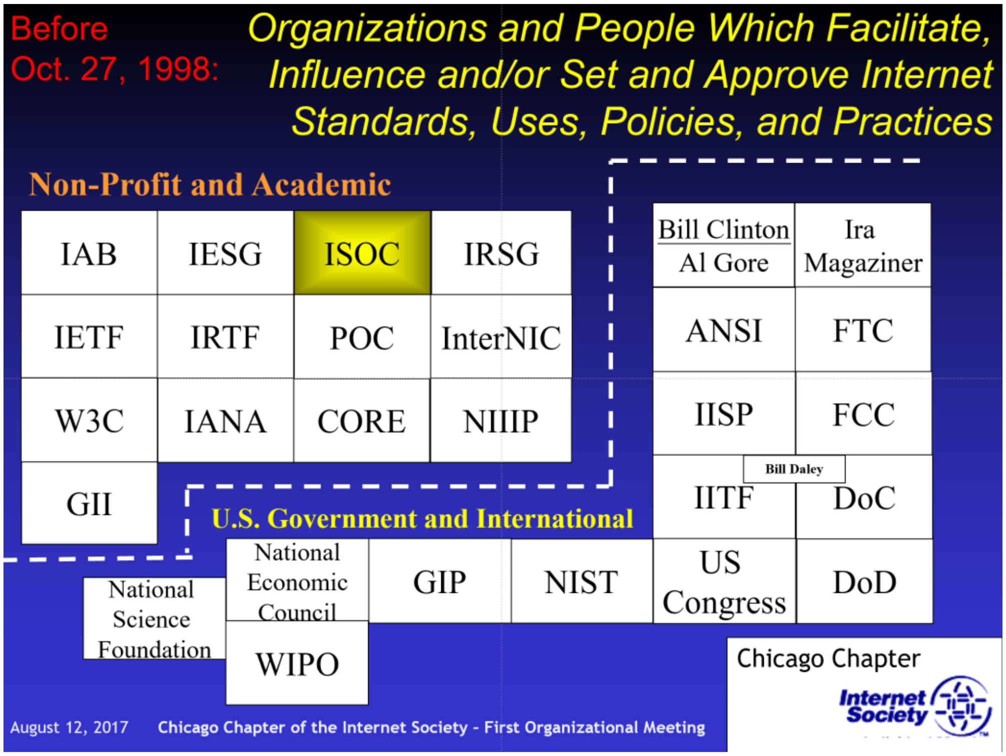


Figure D.1 Internet RFC Publication Process

The diagrams below should the organizations that influence the development of the Internet and Internet Standards. Note that in October 1998, IANA was replaced by ICANN. Also, in 2016, President Obama assigned ICANN as part of the United Nations, so it now operates independently from the authority of the Government of the United States.



Before Oct. 27, 1998:

Organizations and People Which Facilitate, Influence and/or Set and Approve Internet Standards, Uses, Policies, and Practices

Non-Profit and Academic

IAB, IESG, ISOC, IRSG

IETF, IRTF, POC, InterNIC

W3C, IANA, CORE, NIIIP

GII

U.S. Government and International

Bill Clinton, Al Gore, Ira Magaziner

ANSI, FTC

IISP, FCC

IITF, Bill Daley, DoC

US Congress, DoD

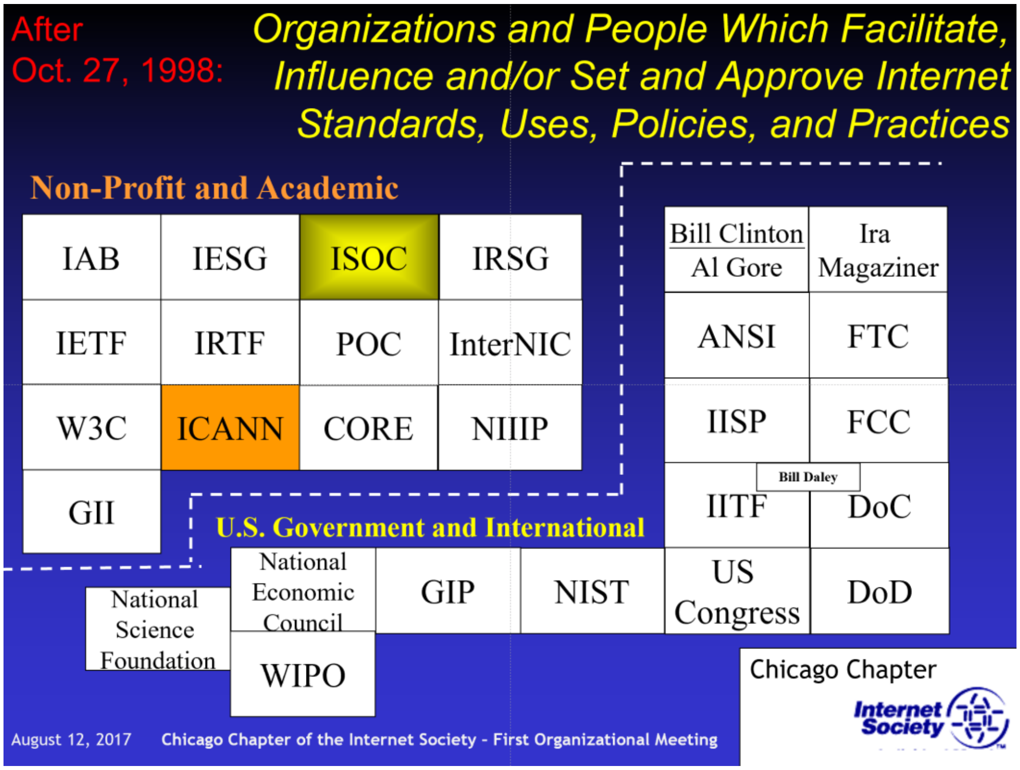
National Science Foundation, National Economic Council, GIP, NIST

WIPO

Chicago Chapter

Internet Society

August 12, 2017 Chicago Chapter of the Internet Society - First Organizational Meeting



After Oct. 27, 1998:

Organizations and People Which Facilitate, Influence and/or Set and Approve Internet Standards, Uses, Policies, and Practices

Non-Profit and Academic

IAB, IESG, ISOC, IRSG

IETF, IRTF, POC, InterNIC

W3C, ICANN, CORE, NIIIP

GII

U.S. Government and International

Bill Clinton, Al Gore, Ira Magaziner

ANSI, FTC

IISP, FCC

IITF, Bill Daley, DoC

US Congress, DoD

National Science Foundation, National Economic Council, GIP, NIST

WIPO

Chicago Chapter

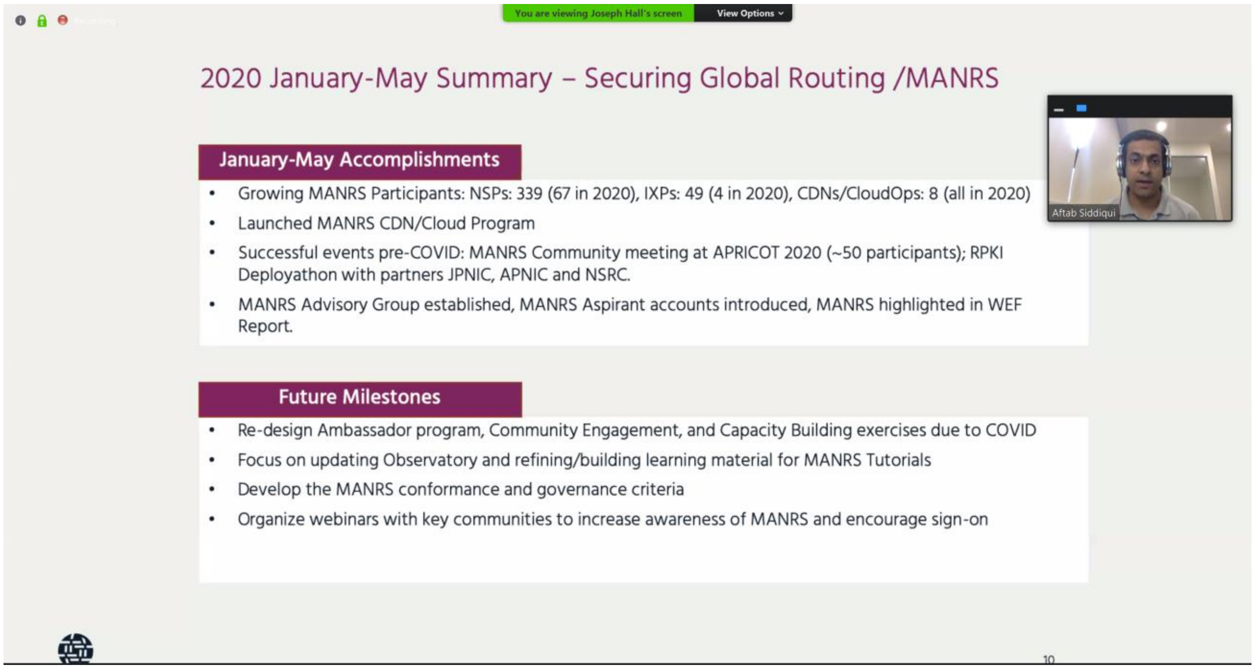
Internet Society

August 12, 2017 Chicago Chapter of the Internet Society - First Organizational Meeting

What Is MANRS?

MANRS stands for the Mutually Agree Norms for Routing Security. It is a collective effort by Internet stakeholders (network operators, content distribution networks and IXPs) needed to achieve global routing security. MANRS has created and published the principles, standards, and procedures for Global Routing Security actions that will provide Routing Security for Global Internet Stakeholders if they are carefully followed. MANRS currently supported by a growing and visible community of more than 200 networks around the world that have adopted the MANRS guidelines for Global Security Internet Routing.

MANRS, is fostered by the Internet Society as a Global Strong Internet Project and it is currently led by Mr. Aftab Siddiqui, who works from Sydney, Australia. The screenshot below from May 5, 2020, shows the status of MANRS initiatives from January 2020 to May 2020, as well as their future plans.



2020 January-May Summary – Securing Global Routing /MANRS

January-May Accomplishments

- Growing MANRS Participants: NSPs: 339 (67 in 2020), IXPs: 49 (4 in 2020), CDNs/CloudOps: 8 (all in 2020)
- Launched MANRS CDN/Cloud Program
- Successful events pre-COVID: MANRS Community meeting at APRICOT 2020 (~50 participants); RPKI Deployathon with partners JPNIC, APNIC and NSRC.
- MANRS Advisory Group established, MANRS Aspirant accounts introduced, MANRS highlighted in WEF Report.

Future Milestones

- Re-design Ambassador program, Community Engagement, and Capacity Building exercises due to COVID
- Focus on updating Observatory and refining/building learning material for MANRS Tutorials
- Develop the MANRS conformance and governance criteria
- Organize webinars with key communities to increase awareness of MANRS and encourage sign-on

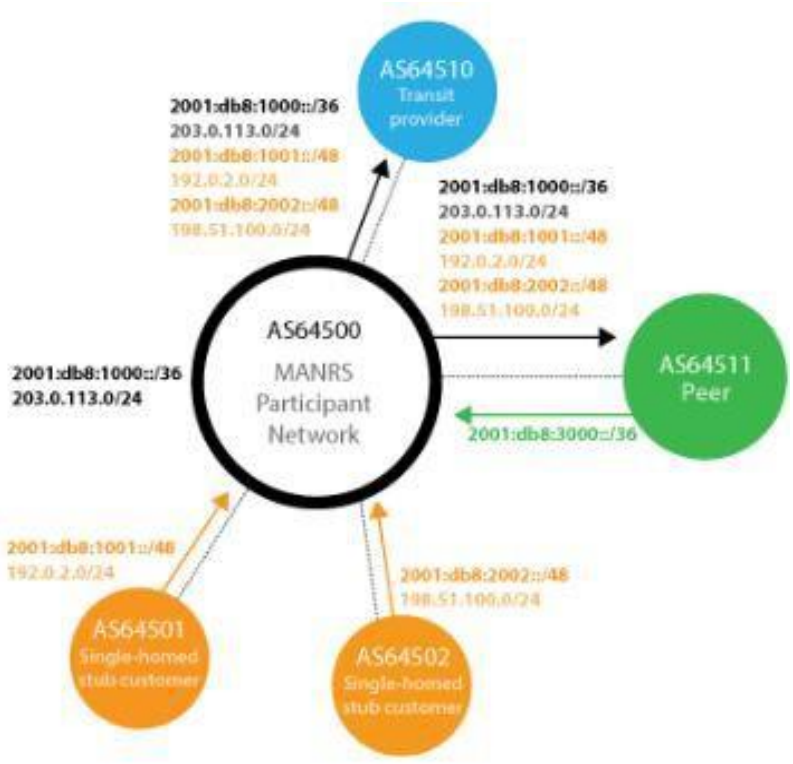
The Internet Society wants more network operators, IXPs and other relevant internet stakeholders to join MANRS to help with the widespread adoption of Global Secure Routing Practice, which will lead to a more robust and secure Internet.

What Problem Does MANRS Address?

When the BPG Internet WAN Routing Protocol was architected, just like the TCP/IP protocol, it was created for accuracy, speed, and efficiency. That's the good news. The bad news is that there are many security issues that BGP does not address. Without addressing Internet security, the raw implementation of BGP routing protocol is subject to many different types of attacks such as spoofing, Distributed Denial of Service (DDoS), reliability, threats to confidentiality of traffic, etc. So think of MANRS as the group of experts who are overseeing the principles, standards, and procedures that address the insecurities that naturally exist in BGP.

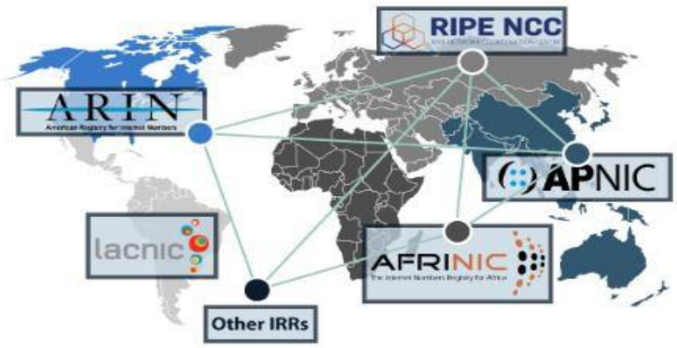
What Is Secure Global Internet Routing?

The idea of Secure Global Internet Routing was created to apply MANRS principles, standards, and procedures to carefully create Network Router Policy descriptor to enable the communication computers called Routers, that route packets on the Global Internet to perform this task as reliably and securely as possible. The diagram below shows the relationship of participant Internet routers that can added to a network infrastructure, with a summary the essential Network Router Policy descriptor objects.



Source: Class 2 Training Materials, ISOC Secure Global Routing Class taught by Dr. Kennedy Ronoh via the web, April 2020 – May 2020.

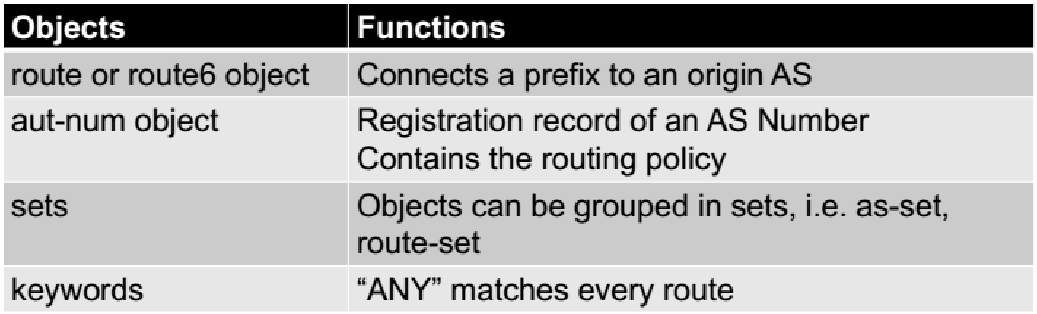
Secure Global Internet Routing Policy Configurations related to the BGP Network Routing Policies defined at an Internet Routing Registry(IRR). The IRRs are shown below:


RIPE NCC
ARIN
American Registry for Internet Numbers
APNIC
lacnic
AFRINIC
The Internet Numbers Registry for Africa
Other IRRs

IRR stands for Internet Routing Registry and is a public database of Internet route objects. IRRs are used for determining and sharing route and other related information used for configuring routers.

Source: Class 2 Training Materials, ISOC Secure Global Routing Class taught by Dr. Kennedy Ronoh via the web, April 2020 – May 2020.

Each IRR has a database that contain entries for the Network Routing Policy entry for each Router that is added into the Global Internet Infrastructure. Each Network Routing Policy comprised of the following objects:



Objects	Functions
route or route6 object	Connects a prefix to an origin AS
aut-num object	Registration record of an AS Number Contains the routing policy
sets	Objects can be grouped in sets, i.e. as-set, route-set
keywords	“ANY” matches every route

Source: Class 2 Training Materials, ISOC Secure Global Routing Class taught by Dr. Kennedy Ronoh via the web, April 2020 – May 2020.

Guidance Proving a 6-Step Summary of the Current Steps Required to Publish a Secure Internet Routing Policy Object.

The Process for Posting your prefixes in Six Easy Steps - From Fremont Cabal Internet Exchange - FCIX. (2018). "A Quickstart Guide to Documenting Your Prefixes with IRR".

1. Create a mntner object (equivalent of a user account) to give you the ability to create IRR objects in your selected IRR database
2. Create an aut-num to represent your autonomous system and describe its contact information (admin and technical) and your routing policy
3. Create an as-set to describe which autonous system numbers your peers should expect to see from you (namely your own and your transit customers)
4. Create a route/route6 object for every prefix originated from your network
5. Update your peeringdb profile to include your IRR peering policy

6. Bask in the glory of enabling your peers to properly filter your peering sessions

Following the MANRS principles, standards and procedures, the creation and application of secure and verified Network Routing Policies and registering these with the IRR that is in the region where the router will reside, helps assure that the Global Internet Infrastructure will be secure, reliable, and continue to grow and evolve in an organized manner that is controllable, will provide the messages to stakeholders in the most efficient manner possible.

Why Secure Global Internet Routing and Why Now?

The importance of entering accurate Network Routing Policy configuration data is underscored by the scale and potential disastrous consequences of that can result from even a single flawed routing misconfiguration on the Global Internet Infrastructure. The paper located at this link: http://www.billslater.com/writing/2002_1107__Internet_Outage_and_Attacks_in_october_2002_by_William_Slater.pdf describes the events and results of what happened when a simple router misconfiguration at WorldCom on the East Coast of the United States led to a series of events that resulted in massive Internet services outages in October 2002. This debacle let to the denial of Internet service for over 40 million people. The root cause analysis of this unfortunate set of events led to improvements in quality controls for accuracy in entering Network Routing Policy Configurations, as well as a plan to increase the security of the Internet Domain Root Servers that existed at time on the Global Internet Infrastructure. In fact, in 2020, the security, reliability, and integrity of the complex global Internet Infrastructure is more important than ever because over 4.6 billion people use the Internet daily (https://www.internetworldstats.com/stats.htm), and 21st century workers and Internet Service consumers are more dependent on the Internet than ever due to events like the international COVID-19 Pandemic Crisis, and the increased universal needs for social distancing and teleworking. Quite simply put, as described in the NASA Mission Control rescue of the of the Apollo 13 in April 1970, we now live in a world where ***“Failure is not an option”.***

What Is Blockchain and Why Is It Important?

Blockchain is like a specialized Operating System that operates on top on Linux, Unix, and of Windows. It stores data in a distributed, decentralized ledger on a peer-to-peer network. All members of a given Blockchain network will have a consistent copy of the distributed ledger technology (DLT) data store. The data is stored in timestamped sequential “blocks” that are append-only, and each block contains the unique hash value of the block that preceded it.   The idea of Blockchain was not exactly invented by Satoshi Nakamoto (Bitcoin inventor) but he popularized it in his 2009, 9-page paper about the creation of the digital currency known as Bitcoin. Below is a diagram from that paper:

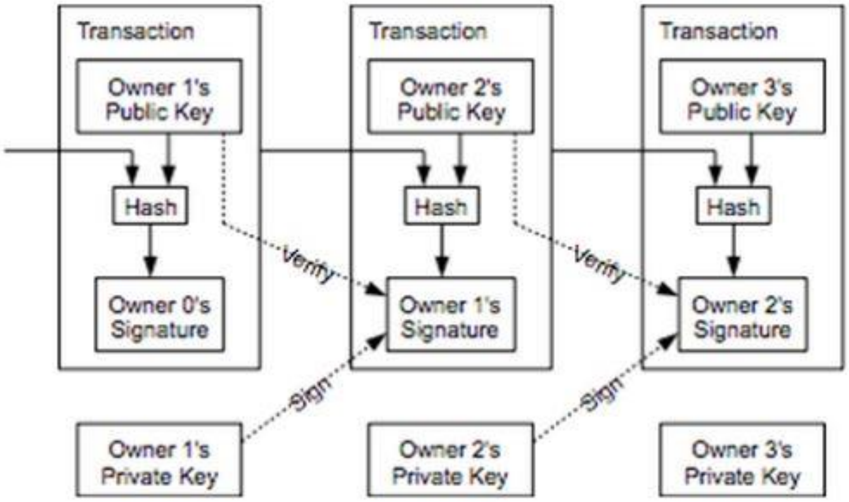


Image: Satoshi Nakamoto

In addition to hashing, Blockchain uses Public-Key Cryptography to secure the data in each block on the Blockchain DLT. Because of the way the Blockchain architecture works, new data can only be appended to the end of the Blockchain and there are no deletes of modifications allowed to the data. Data on Blockchain DLTs is said to be immutable because it cannot be changed. Two of the most common Blockchains, Bitcoin and Ethereum, are in Open Source Code and available on Github.

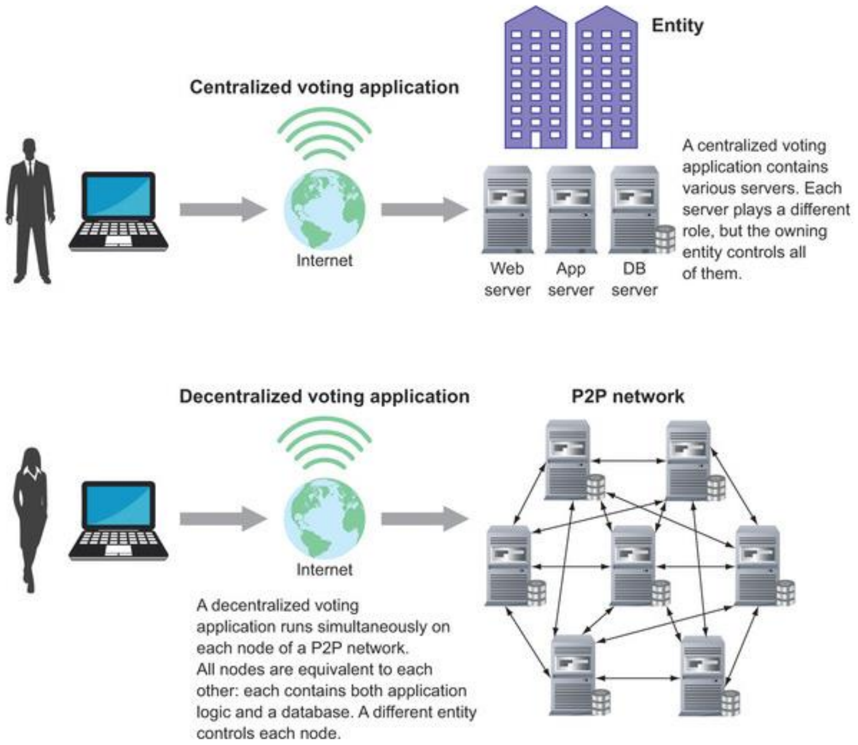
There are two types of Blockchain nodes on a peer-to-peer Blockchain network, clients and miners. Both of these are always supposed to have a current copy of the the DLT, but the miner nodes collect transaction data and assemble it into "blocks". Blockchain is driven by a consensus protocol, which is a form of agreement. Two examples of consensus protocols are Proof of Work, and Proof of Stake.

Blockchain is important because it is being widely adopted for trusted computing, especially in the areas of supply chain management, financial industry, the legal industry, healthcare, business, education, and many other areas of the business world. In 2019, U.S. Congress introduced a Bill in July 2019, the Blockchain Promotion Act of 2019. Other key benefits are that Blockchain reduces risk of computer fraud, and this makes it a real business enabler.

Note that Blockchain IS NOT Cryptocurrency, BUT Cryptocurrency uses Blockchain.

The diagram below shows the comparison between a decentralized Blockchain Network and a Centralized Voting System Network.

Figure 1.2. Comparison of a centralized voting application with a decentralized one. One institution owns all servers of a centralized application. A decentralized voting application runs simultaneously on multiple nodes of a network that different entities own.


Entity
Centralized voting application
Internet
A centralized voting application contains various servers. Each server plays a different role, but the owning entity controls all of them.
Web server
App server
DB server
Decentralized voting application
P2P network
Internet
A decentralized voting application runs simultaneously on each node of a P2P network. All nodes are equivalent to each other: each contains both application logic and a database. A different entity controls each node.

Source: Roberto Infante, Building Ethereum DApps, 2019

How Can Blockchain Enhance Secure Global Routing?

Using Blockchain Distributed Ledger Technology to provide the storage of Network Routing Policy data in a Distributed Ledger that is both immutable and decentralized, will provide these advantages:

- Provide the important Network Routing Policy configuration data in the sequential, timestamped, immutable DLT data store.
- Create a history of Network Routing Policy configuration data that can be quickly accessed by any authorized engineer for troubleshooting purposes.
- Streamlining the efforts required to perform the current steps required for creating Network Routing Policy configuration.

- Have the possibility of providing this data or perhaps combining it for use with the other regional Internet Routing Registries.

Conclusion

Though this is an original idea for Secure Global Internet Routing Configuration with entering Network Router Policy information on an immutable, decentralized distributed ledger, this is not the first time that a Blockchain-based solution has been proposed to help secure the Internet Infrastructure. In July 2018, at Trinity College in Dublin. Ireland, Ms. Scarlett Gourley, a graduate student, and her Professor, Dr. Hitesh Tewari, co-authored their seminal study and paper on "Blockchain-based DNSSEC". This paper is readily available for reference here at this link: https://www.researchgate.net/publication/326489781_Blockchain_Backed_DNSSEC.

The advantage of the proposed Blockchain DApp will be to provide rapid widespread secure access to immutable, decentralized data that will serve as an authoritative record of the time-stamped sequence of transactions made to update the Global Internet Infrastructure, and to document and provide a secure, decentralized single source of truth that can be used by multiple networking engineers and managers from geographically distributed locations to rapidly reconstruct Router Configurations related to Network Router Policy additions and changes (updates that supersede previously existing Network Router Policy data). Access to such data will help multiple technical stakeholders to rapidly collaborate to identify the Internet Infrastructure change history, and to pinpoint and hopefully resolve any possible errors that could result in outages and/or incorrectly routed Internet traffic.

It is unclear if the design ideas documented in my Project Blog will ever result in a real-life Ethereum Blockchain DApp that would be widely adopted by any or all of the IRRs, but the concepts discussed will serve to show the importance, viability, and advantages of such a solution.

Important Resources for Your Success

Internet Routing Resources

ARIN’s IRR User Guide

BGPStream by Cisco. https://bgpstream.com/

Fremont Cabal Internet Exchange - FCIX. (2018). "A Quickstart Guide to Documenting Your Prefixes with IRR". An article published by FCIX and retrieved from https://fcix.net/whitepaper/2018/07/14/intro-to-irr-rpsl.htmlon May 4, 2020.

IRR Explorer - A remarkably handy tool for generating a dashboard of your current IRR status compared to what’s seen on BGP coming from your network

RFC2622 - “Routing Policy Specification Language (RPSL)”: Describes the basic RPSL object syntax

RFC3704 - "Ingress Filtering For Multihomed Networks"

RFC4012 - “Routing Policy Specification Language next generation (RPSLng)”: Describes useful additions to the RPSL language such as IPv6 route6 objects

RFC2650 - “Using RPSL in Practice”: A tutorial on generating RPSL objects

RFC7682 - “Considerations for Internet Routing Registries (IRRs) and Routing Policy Configuration: Some of the problems and lessons learned about the IRR system

RIPE’s Documentation on using PGP to authenticate mntner objects: In case you’d like to use more robust authentication.

Blockchain Resources

Several Presentations on Blockchain, Blockchain Security, and Blockchain Development: http://billslater.com/writing.

Bitcoin Resource Page: http://billslater.com/bicoin.

Blockchain Resource Page: http://billslater.com/blockchain.

References

451 Research. (2017). MANRS Enterprise Use Cases - A White Paper published October 16, 2017 by 451 Research. Retrieved from isoc.box.com/s/fpoqnmvjd9unuicxlrtp2uj89c0fihi6 on April 21, 2020.

Antonopoulos, A. M. (2018). Mastering Bitcoin: Programming the Open Blockchain, second edition. Sebastopol, CA: O'Reilly Media, Inc.

Antonopoulos, A. M. and Wood, G. (2019). Mastering Ethereum: Building Smart Contract sand DApps. Sebastopol, CA: O'Reilly Media, Inc.

Bahga, A. and Madisetti, V. (2017). Blockchain Applications: A Hands-On Approach. Published by Arshdeep Bahga and Vijay Madisetti. www.blockchain-book.com .

Bambara, J. J. and Allen P. R. (2018). Blockchain: A Practical Guide to Developing Business, Law, and Technology Solutions. New York, NY: McGraw-Hill Education.

Bashir, I. (2018). Mastering Blockchain, second edition. Birmingham, UK: Packt Publishing Ltd.

Bitcoin.org. (2014). Bitcoin.org FAQs. Retrieved from https://bitcoin.org/en/faq on April 10, 2014.

Blockchain Training Alliance. (2019). Global Blockchain Terms, version 2.0. Retrieved from https://cdn.shopify.com/s/files/1/2137/1081/files/BTA_Global_Blockchain_Terms.pdf?2499 on August 14, 2019 .

Casey, M. J. and Vigna, P. (2018). The Truth Machine: The Blockchain Reference and the Future of Everything. New York, NY: St. Martin's Press.

Caughey, M. (2013). Bitcoin Step by Step, second edition. Amazon Digital Services.

References

Champagne, P. (2014). The Book of Satoshi: The Collected Writings of Bitcoin Creator Satoshi Nakamoto. Published by E53 Publishing, LLC.

Dannen, C. (2017). Introducing Ethereum and Solidity: Foundations of Crytocurrency and Blockchain Programming for Beginners. New York, NY: Apress

De Filippi, P. and Wright, A. (2018). Blockchain and the Law: the Rule of Code. Cambridge, MA: President and Fellows of Harvard College.

De Havilland, P. (2018). Greedy, Prodigal, and Suicidal — Hosho to Save Smart Contracts From Three Deadly Sins. An article published at Bitsonline.com on September 3, 2018. Retrieved from https://bitsonline.com/greedy-prodigal-suicidal-hosho-smart-contracts/ on February 27, 2019.

Dhillon, V., Metcalf, D., and Hooper, M. (2017). Blockchain Enabled Applications: Understand the Blockchain Ecosystem and How to Nake It Work for You. New York, NY: Apress.

Drescher, D. (2017). Blockchain Basics. Frankfort am Main, Germany: Apress.

Eddison, L. (2017). Ethereum: A Deep Dive into Ethereum. Published by Leonard Eddison.

Etwaru, R. (2017). Blockchain Trust Companies. Indianapolis, IN: Dog Ear Publishing.

Ferry, T. (2019). To Blockchain or not to Blockchain. An article published at Medium.com on June 8, 2018. Retrieved on January 13, 2019 from https://medium.com/causys/to-blockchain-or-not-to-blockchain-aed05bf08150 .

Fremont Cabal Internet Exchange - FCIX. (2018). "A Quickstart Guide to Documenting Your Prefixes with IRR". An article published by FCIX and retrieved from https://fcix.net/whitepaper/2018/07/14/intro-to-irr-rpsl.htmlon May 4, 2020.

Gerard, D. (2107), Attack of the 50 Foot Blockchain: Bitcoin, Blockchain, Ethereum, and Smart Contracts. Published by David Gerard. www.davidgerard.co.uk/blockchain.

Gourley, S. and Tewari, H. (2018). Blockchain-based DNSSEC. Trinity College, Dublin, Ireland. Retrieved from https://www.researchgate.net/publication/326489781_Blockchain_Backed_DNSSEC on July 30, 2018.

GreenBerg, A. (2019). A Blockchain Bandit Is Guessing Private Keys and Scoring Millions, An article published on April 23, 2019 at Wired.com and retrieved from https://www.wired.com/story/blockchain-bandit-ethereum-weak-private-keys/ on April 23, 2019.

Incencio, R. (2014). Ransomware and Bitcoin Theft Combine in BitCrypt. Retrieved from http://blog.trendmicro.com/trendlabs-security-intelligence/ransomware-and-bitcoin-theft-combine-in-bitcrypt/ on March 27, 2014.

Infante, R. (2019) Building Ethereum DApps. Shelter Island, NY: Manning Publications.

Laurence, T. (2017). Blockchain for Dummies. Hoboken, NJ: John Wiley & Sons, Inc.

Lee, T. B. (2013). 12 questions about Bitcoin you were too embarrassed to ask. Retrieved from http://www.washingtonpost.com/blogs/the-switch/wp/2013/11/19/12-questions-you-were-too-embarrassed-to-ask-about-bitcoin/ on November 19, 2013.

Ma, M. (2017). Blockchain Design Sprint: An Agile Innovation Workbook to Implement an Agile Design Sprint for your Blockchain Business. Published by Future Lab www.futurelabconsulting.com.

MANRS. (2017). Mutually Agreed Norms for Routing Security (MANRS) Implementation Guide, version 1.0 Retrieved on April 14, 2020 from https://www.manrs.org/isps/guide/.

Markowitz, E. (2014). Cryptocurrencies Are the New Spam Frontier. Retrieved from http://www.vocativ.com/tech/bitcoin/cryptocurrencies-new-spam-frontier/ on March 28, 2014.

Nakamoto. S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from https://bitcoin.org/bitcoin.pdf on November 1, 2013.

Nguyen, J. (2019). Blockchain still vulnerable to hacks despite security hype, but here are some solutions. Retrieved from https://e27.co/blockchain-still-vulnerable-to-hacks-despite-security-hype-but-here-are-some-solutions-20190212/ on February 13, 2019.

O'Ham, T. (2018). Singapore Research Team Codifies 3 new Ethereum VM Vulnerabilities. An article published at Bitsonline.com on February 21, 2018. Retrieved from https://bitsonline.com/singapore-research-ethereum/ on February 27, 2019.

Orcutt, M. (2019). Once Hailed as Unhackable, Blockchains Are now Getting Hacked. An article in MIT Review. Published February 19, 2019. Retrieved from https://www.technologyreview.com/s/612974/once-hailed-as-unhackable-blockchains-are-now-getting-hacked/ on February 24, 2019.

Popper, N. (2013). Into the Bitcoin Mines, Retrieved from http://dealbook.nytimes.com/2013/12/21/into-the-bitcoin-mines/?hp&_r=0 on December 21, 2013.

Prusty, N. (2017). Building Blockchain Projects: Building Decentralized Blockchain Applications with Ethereum and Solidity. Birmingham, UK: Pact Publishing.

Ramone, A. D. (2019). How to Secure a Blockchain: 3 Things Business Leaders Know. An article published at Techrepublic.com on April 18, 2019. Retrieved from https://www.techrepublic.com/article/how-to-secure-a-blockchain-3-things-business-leaders-need-to-know/ on April 23, 2019.

Randall, I. (2020). Global internet outages reach a record high during the coronavirus lockdown as broadband operators tinker with networks to meet increased demand from people working from home. Published April 29, 2020 at Daily Mail UK. Retrieved from https://www.dailymail.co.uk/sciencetech/article-8269245/Global-internet-outages-reach-record-high-coronavirus-lockdown.html on April 30, 2020.

SCGNEWS. (2014). The IRS Just Declared War on Bitcoin - Retroactively. Retrieved from http://scgnews.com/the-irs-just-declared-war-on-bitcoin-retroactively on March 27, 2014.

Schudel, G. and Smith, D.J. (2008). Router Security Strategies: Securing IP Traffic Planes. Indianapolis, IN: Cisco Press.

Sharkey, T. (2014. Inside Bitcoins NYC Day 1: Bitcoin 2.0 Takes Center Stage. Retrieved from http://www.coindesk.com/inside-bitcoins-nyc-day-1-bitcoin-2-0-takes-center-stage/ on April 8, 2014.

Slater, W. F. (2002). The Internet Outage and Attacks of October 2002. Retrieved from http://www.billslater.com/writing/2002_1107__Internet_Outage_and_Attacks_in_october_2002_by_William_Slater.pdf on May 1, 2020.

Smith, B. (2019). The Evolution of Cryptocurrency in Terrorism. Retrieved from Blockchain Training Alliance. (2019). Global Blockchain Terms, version 2.0. Retrieved on August 14, 2019 from https://www.bellingcat.com/news/2019/08/09/the-evolution-of-bitcoin-in-terrorist-financing/ on August 10, 2019.

Xu, X., Weber, I, and Stables, M. (2019). Architecture for Blockchain Applications. Nature, Switzerland: Springer Publications.

Zenko, M. (2017). Bitcoins for Bombs – a Blog published at the Council on Foreign Relations on August 17, 2017. Retrieved from https://www.cfr.org/blog/bitcoin-bombs on February 13, 2019.