Blockchain for BGP

https://datatracker.ietf.org/doc/draft-mcbride-rtgwg-bgp-blockchain/

D. Trossen, D. Guzman, M. McBride, T. Martin

Goal for this Draft

Review possible **opportunities** of using *Distributed Consensus Systems* (DCSs) to secure BGP policies within a domain and across the global Internet

Propose that BGP data could be placed in a DCS and smart contracts can **control how the data is managed**

Create a **single source of truth**, something for which DCSs are particularly well suited, as a **complement** to existing IRR and RPKI mechanisms

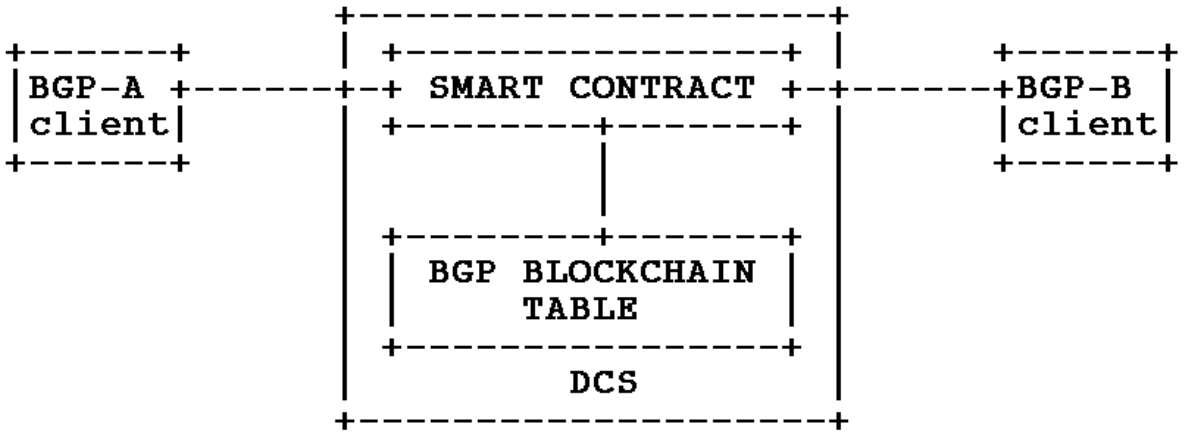
Structure of this Draft and Changes since IETF116

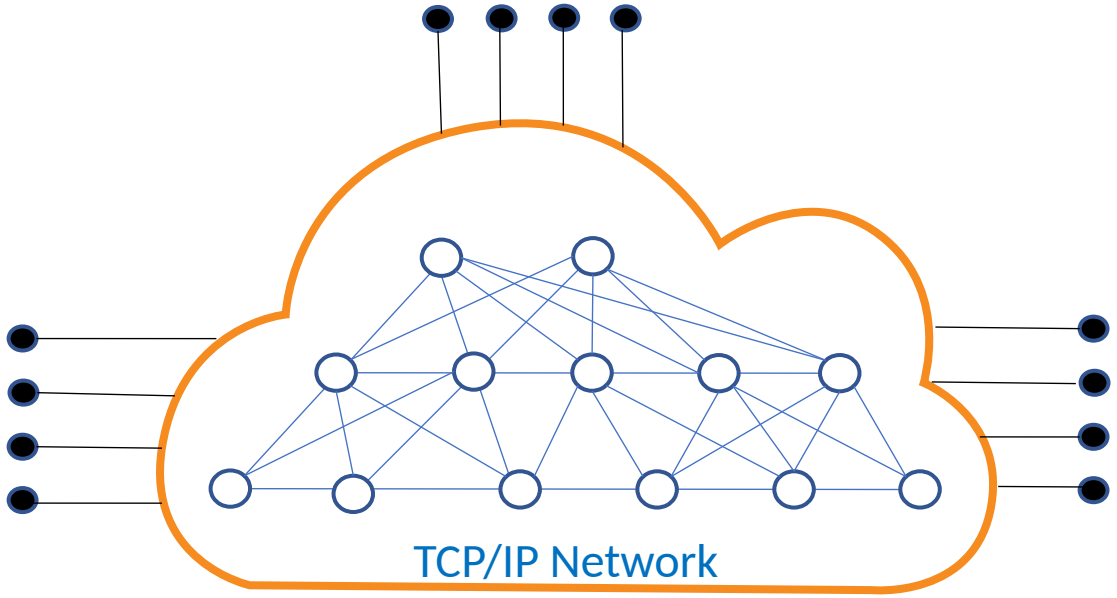
1. Introduction 2
2. A Strawman for a simple BGP Distributed Consensus System . . 3
3. Opportunities for Using DCSs for BGP 5
   3.1. Preventing fraudulent BGP origin announcements 5
   3.2. Validating incoming BGP updates 5
   3.3. Providing routing policy such as QoS 6
   3.4. Protecting BGP files 6
   3.5. Providing path validation 6
   3.6. Securing BGP Controllers 7
   3.7. Securing Blockchain compromised by BGP vulnerabilities . 7
4. Key Challenges for a BGP DCS 7
   4.1. DCS Convergence Latency 8
   4.2. Communication Costs 10
   4.3. Working on Inconsistent State 11
5. Possible Solution Technologies 11
   5.1. Routing on Service Addresses 12
   5.2. Compute-Aware Traffic Steering 13
   5.3. Locator/ID Separation Protocol 13
6. Conclusions 13

- Added Thomas Martin as **co-author**.
- Added **key challenges** to be addressed by a possible BGP DCS
  - Update latency
  - Costs (for communication)
  - Working on inconsistent state
- Outlined **possible networking solutions** to contribute to addressing those challenges
  - Routing on Service Addresses (ROSA)
  - CATS
  - LISP

Bit of Background

- **Smart contracts** are programs realizing BGP-related operations and store their (distributed) state in a DCS
  -> A DCS could be used to supplement existing BGP management
- A **BGP related smart contract** could be executed when some condition such as receiving an update with too many prepends or hijacking detection
- DCS realized through a **P2P Network** where participating nodes verify transactions, execute smart contracts, boot/seed nodes to bootstrap clients/new nodes, process new blocks, full nodes,lightweight nodes…





Potential BGP Opportunities

- Avoiding fraudulent BGP origin announcements
- Validating incoming BGP updates
- Providing routing policy such as QoS
- Protecting BGP config files
- Providing path validation
- Securing BGP Controllers
- Securing Blockchain compromised by BGP vulnerabilities
- BGP functional resilience and reliability

Key Challenges

- Convergence Latency
  - Convergence here is to achieve **majority rule** of any state change in DCS
  - P2P nature of DCS leads to **significant latency issues**, particularly for a cold start

  -> need to **identify key latency bounds** for BGP use cases and **evaluate technology landscape** to meet them
- Communication Costs
  - P2P nature of DCS requires dealing with **reachability, availability,** and **suitability** of (distributed) peers

  -> lots of probing and capability exchange happening

  -> **high costs** and **impact** on provider networks
- Working on Inconsistent State
  - Lack of (fast) consensus leads to methods for proof of inconsistent state

  -> is notion of inconsistent state **acceptable**?

  -> are proof methods **viable** (economically as well as latency wise)?

Separately reported in

- draft-trossen-rtgwg-impact-of-dlts
- Guzman, D., Trossen, D., McBride, M., and X. Fan, "Insights on Impact of Distributed Ledgers on Provider Networks", Paper Blockchain – ICBC 2022, 2022.

Possible Relevant Solution Technologies

- Routing on Service Addresses (https://datatracker.ietf.org/doc/html/draft-trossen-rtgwg-rosa)
  - Interpret DCS as a **service environment**, where peers are **service instances** of key services:
    - *Insertion* service (for inserting new state into the DCS)
    - *Diffusion* service (for diffusion new state for convergence)
    - *Query* service (for querying the latest consented state)
  - Routing to a number of service instances is one of **anycast/diffusion distribution**
  - Reachability and availability in current DCSs replaced by (service) **routing announcement** and **aggregation**

  -> **lower costs** and possibly **faster diffusion** to improve on latency and cost challenges
- Compute-Aware Traffic Steering (https://datatracker.ietf.org/wg/cats/about/)
  - Computational awareness may lead to **capability-rich diffusion** policies (e.g., diffuse to less loaded or well-connected peers)

  -> complement service routing approach in certain use cases to possibly further **accelerate diffusion**
- LISP
  - Use EID/locator separation
  - TBD through future discussions with community

Summary & Next Steps

- Smart contracts are **programs** executed within a DCS
  - A BGP DCS could provide **distributed state/information** management for those BGP smart contracts
- Extended identified **opportunities** with **key challenges** when realizing DCS for BGP
  - Latency may prevent use of DCS
  - Costs may make DCS prohibitive, both in applicability and sustainability
- Identified first set of **possible network technologies** that may address challenges
  - Looking a DCS as a compute-aware service environment may be a useful area of investigation

  -> possible future **use case draft** for ROSA and CATS?

- **Important**: we need **more input** from the wider community
  - **Network experts** to help us tease out challenges to applicability and technologies
  - **DCS experts** to align with the latest state-of-the-art

Please join us at dlt-networking@ietf.org for the dialogue on this topic