BGPChained

Adelaida von der Full, Enin Savier, Wesley Gryffindor

April 13, 2026

(adelae.vonderfull@protonmail.com) (enin.savier@protonmail.com) (wesley.gryffindor@protonmail.com)

Abstract

This project proposes BGP extension that would provide Integrity, Authenticity and Availability of AS metadata as well as security enchancement. It is achieved via application of Distributed Ledger Technlogy to the AS metadata. Security achieved via application of cryptography in the link establishing process. The project has the potential to reorganize and unify AS management as well as address space management across globe.

1 Introduction

Current InterNet relies heavily on BGP version 4 that was introduced long time ago. It is primary protocol to distribute information about interconnected networks. At the time it was introduced, there ware not so many services of huge financial value relying on it and compute power of ordinary hardware of that era was not capable of hadling strong data validation. So as of now the network relies heavily on trust.

Things have changed a little since the inception of the InterNet. Current InterNet connectivity represent blood vessels of the worldwide‘s economy. Simple principle says that treasure storage should worth about tenth of the stored value. Thus InterNet should have some measures to validate correctness of metadata BGP gets and distributes. Even at the expense of consumed computational resources. To be fair, the trust is mitigated by regional authorities to some extent and there ware numerous attempts to apply some checks to the protocol(RPKI, ROA, ASPA) but adoption of the methods mentioned is far from dominant.

The InterNet gave a birth to the Distributed Ledger Technology, which provides Integrity, Authenticity and Availability. Nice properties that should be incorporated in the BGP protocol be able to introduce some level of confidence in current InterNet. This paper proposes slight changes to the BGP protocol itself as well as approaches to the organistion of Autonomous Systems and address space management using DLT and cryptography to achieve desired properties as well as migration playbook.

2 Migration

To make transition from existing system there should be mechanism for participants of the InterNet network to show their concent to participate in the proposed project. This shold be possible by adding comment to the Routing Description of the AS with the public key in it.

There should be some mechanism to transfer data from regional registries to the proposed project. To be able to validate data regarding ownership and leases of prefixes between ASes there should be pool of validators that are parsing state regularly and collectively submit transactions regarding changes, and, depending on, if the owner is participant or not, submit it with consensus or leave it to the owner of the resource (similar to chainlink).

2.1 2/3 lockin

Once the project would be signaled by the majority of AS owners it is possible to collectively decide if the project may be considered source of truth for routing info and address space management. This would require voting mechanism.

2.2 Voting of the participants

It is possible to organaze voting on DLT using simple set of data: ballot topic, ballot type, timeframe and AS owner's acceptance or denial. It should be possible to calculate if proposed ballot topic is accepted or denied by collecting the data from the DLT.

3 Timestamp server

To make universal clock for all the transactions submitted, there should be some mechanism like block height to make order of events, as basically every change to addresses set of data is very sensetive to lifespan of the lease after lockin. The lifespan of the lease is calculated as difference of the current height of the block and the height of the block where it was included.

4 Transactions

In order to map current information regarding network state two different sets of data needed. One for mapping AS number to prefix operated by it, second for connection between two ASs. First one should not update frequently so it fits just fine within current DLT implementations, second is a bit trickier. It should reflect if one AS lost connection to other AS, for others to make changes in the routes as fast as possible.

To make changes in the first set of data criptographicaly signed transaction needed. The transaction should contain at least one mechanism for collective majority to revoke it, and at least one mechanism to track lease time for it. As

in publicly shared address space one malicious participant can make significant impact. The transactions may be processed in batches or one by one.

To make changes in the second set cryptographicaly signed transaction from both sides needed to estrablish connection and signed from any side transaction needed to notify state update of the connection. Just like Lightning Network does.

4.1 Transaction structure

Every transaction in those 2 sets of data should be revokable by the majoity of the patcipants. To achieve this, transaction signature should be specifically crafted: the signature itself is a cryptographycaly signed abstract sintax tree, leafs of which would represent 3 cases:

- The public key of the sender could do manipulations to the entry if balance is greater than zero.
- The validators could reclaim the entry if the balance is zero.
- The majority vote can reclaim it if the voting was conducted and received approvals of 2/3 of participants.

Second and third case would be available only after 2/3 of the AS would join proposed project as there is inability to use lease expiry until majority of ASes and corresponding address space would be locked inside the proposed project. It may require some form of voting to enable lease expiry after majority of the network participants would join.

4.2 Transactions before 2/3 lockin

Before lockin every record in local registries (RIPE, ARIN, etc) considered valid. To be able to reflect changes in registries the participant AS should send transactions in DLT with the changes made.

To be able to validate that no 2 participants own same prefix all address space should be reflected in the DLT. It would allow to mitigate announcing random prefixes on behalf of other AS attack.

The validators majority can sign specially crafted transaction which allows new participant to gain access to the resources already reflected in DLT.

4.3 Transactions after 2/3 lockin

After lockin the balance of every public key reflecting AS inflates equal amount every block and if balance became zero the validators would be able to reclaim that AS and address space allocated to it into available for lease address space.

4.4 Realtime state updates transaction

When any peer is offline or decided to tear-down the link it sends update transaction to the network signed with the key that was used for establishing link. By doing it this way it is possible to have verified peering info in sync with links.

4.5 Voting transactions

To create a voting the should be specifically crafted transaction with three variables: ballot type, ballot topic (description), and time-frame in form of block height and it should be signed by the initiator of the vote.

To participate in the voting AS owners would sign transactions regarding ballot with their opinion. For every ballot there should be distinct identifier inside the transaction as well as expressed opinion regarding the ballot.

Unlike transactions for AS metadata, voting transactions is cryptographically signed by the AS owner‘s key.

5 Pricing policy

Currently, LIR (registry representative) is deciding which amount to charge for the AS record to be present in the registry. The pricing for the address block is decided by the owner of the address block as there is no free address space in IPv4.

There should be simple pricing policy equal for all AS owners after the 2/3 lockin:

> The policy states that price for every new assigned address block rises proportional to square of number already assigned blocks. Address block is defined as 256 IPv4 addresses. This policy would reclaim all unused address space into available for lease and would incentivize not to squatt more address space for AS than required for current needs.

Example: AS with 1 block pays n per block height difference, AS with 2 blocks pays (1+4)*n per block height difference, AS with 3 blocks pays (1+4+9)*n per block height difference. Where “n” is some amount that would be decided by the participants of the project.

6 Network

To exchange information between participants there should be some mechanism like network of connected nodes. The nodes may be of different types, some should mainly utilize both sets of data, some should validate transactions and assemble blocks for first set of data, some should check all existing transactions for expiry.

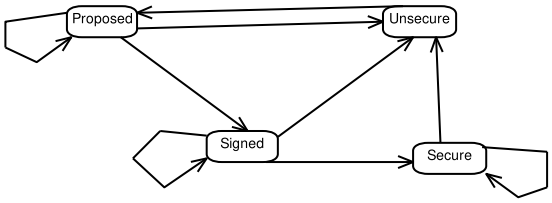

Figure 1:
Additional state machine for BGP connection state

BGP itself is a communication protocol capable of delivering messages through the InterNet. So with slight modifications it is possible to add extra duty to it. What if we extend BGP neighbor state machine with few extra states? Assuming that existing network operates using standard protocol, introduction of new states should not break anything. Taking that into count we can only incorporate new states after the connection established state. After the connection is in established state it is possible to propose peer to open secure connection and if it reaches secure state the peer runs same protocol. Otherwise connection state would settle in unsecure state.

Introduction of differentiation between secure and unsecure connections gives the ability to re-weight existing routes and build secure routes with the ability to fallback to unsecure when the desired destination is unreachable via secure path.

Once BGP connection is in secure state it is posable to send additional fields in the update messages to be able to fetch and distribute transaction updates. This mechanism provides channel to funnel updates across network until saturation.

Until secure connections network graph reaches connectivity there should be possibility to make secure tunnels between participants of BGPChained to be able to get transaction updates regarding link security state.

7 Incentive

In order to convince owners of ASes to participate and deploy proposed project there should be some form of material motivation. For those that validate data and collect it from external sources there should be compensation proportional to the amount of work made.

For the AS owners main benefit reveals after 2/3 lockin, as it would be possible to make fees equal for every AS of the InterNet. Same goes for the address space.

After 2/3 lockin, the procedure of joining InterNet would be somewhat different: the network owner would find nearby AS owners and ask them to open connection with new AS which would be tied to public key address in the DLT with some positive balance. Once connections would be opened, the transactions would appear in the DLT. To make announcement of the address range for

new AS, the address block should be leased from the available (reclaimed) address space by crafting transaction that claims it. As long as balance is positive the network would participate in the InterNet.

8 Calculations

Currently, the distribution of AS numbers and ip addresses is shaped by the past evolution of the internet:

Rank	Country	Code	Number	Percentage
1	United States	US	31 849	26.360 %
2	Brazil	BR	9 157	7.579 %
3	China	CN	6 597	5.460 %
4	India	IN	6 166	5.103 %
5	Russian Federation	RU	5 735	4.747 %
6	Indonesia	ID	3 852	3.188 %
7	Germany	DE	3 181	2.633 %
8	United Kingdom	UK	3 088	2.556 %
9	Australia	AU	2 971	2.459 %
10	Canada	CA	2 482	2.054 %
11	Poland	PL	2 449	2.027 %
12	Ukraine	UA	2 005	1.659 %
13	Bangladesh	BD	1 973	1.633 %
14	France	FR	1 852	1.533 %
15	Netherlands	NL	1 582	1.309 %
16	Argentina	AR	1 330	1.101 %
17	Hong Kong	HK	1 315	1.088 %
18	Italy	IT	1 296	1.073 %
19	Japan	JP	1 292	1.069 %
20	Korea, Republic of	KR	1 175	0.972 %

Table 1: Top 20 countries by AS number count

Rank	Country	Code	Number	Percentage
1	United States	US	1 608 628 640	43.625 %
2	China	CN	342 952 192	9.301 %
3	Japan	JP	188 678 976	5.117 %
4	United Kingdom	UK	140 402 688	3.808 %
5	Germany	DE	126 266 176	3.424 %
6	Korea, Republic of	KR	112 494 336	3.051 %
7	France	FR	81 738 064	2.217 %
8	Brazil	BR	79 978 496	2.169 %
9	Canada	CA	67 632 384	1.834 %
10	Italy	IT	53 916 032	1.462 %
11	Netherlands	NL	47 826 656	1.297 %
12	Australia	AU	46 116 096	1.251 %
13	Russian Federation	RU	45 048 128	1.222 %
14	India	IN	41 890 560	1.136 %
15	Taiwan, Province of China	TW	35 721 984	0.969 %
16	Spain	ES	32 112 256	0.871 %
17	Sweden	SE	31 367 456	0.851 %
18	Mexico	MX	28 952 832	0.785 %
19	Singapore	SG	27 403 264	0.743 %
20	South Africa	ZA	27 156 736	0.736 %

Table 2: Top 20 countries by IPv4 address space

Rank	Country	Population	GDP-per-capita IMF 2026 in USD	Ipv4 addresses	Ipv4-per-person percentage
1	India	1476625576	3051	41890560	2.83691%
2	China	1412914089	14730	342952192	24.27269%
3	United States	349035494	92883	1608628640	460.87824%
4	Indonesia	287886782	5398	19233792	6.68103%
5	Pakistan	259299791	1707	5441536	2.09855%
6	Nigeria	242431832	1378	3197696	1.31901%
7	Brazil	213562666	10709	79978496	37.44966%
8	Bangladesh	177818044	2960	2069056	1.16358%
9	Russia	143394458	17287	45048128	31.41553%
10	Ethiopia	138902185	1124	370176	0.26650%
11	Mexico	132997658	15111	28952832	21.76943%
12	Japan	122427731	36391	188678976	154.11457%
13	Egypt	120101175	3579	24150528	20.10849%
14	Philippines	117724471	4619	6248448	5.30769%
15	DR Congo	116452162	2542	182016	0.15630%
16	Vietnam	102177431	4965	16489728	16.13833%
17	Iran	93168497	4250	10819584	11.61292%
18	Turkey	87926082	18232	16791168	19.09691%
19	Germany	83644258	63600	126266176	150.95618%
20	Tanzania	72563780	1378	1094400	1.50819%

Table 3: Top 20 countries by population

What would happen after lockin if major address space holders would not be able to prolonge their leases? Lets imagine that price for 256 address block lease would be 0,025 US cents per month. To be able to maintain 1000 blocks it would be 332833500 times 0,025 or 83208.375 USD per month. Lets assume that address utilization is 33%. Given that assumption AS owners with address space exciding 1000 blocks would be required to charge roughly 1 USD per month for 1 IP address. If this holds as true AS owners with more then 4000 blocks would be required to charge roughly 16 USD per month for 1 IP address. So the AS with high number of IP addresses would reduce address space and pool of freed-up addresses would allow new ASes to join InterNet.

Rank	Country	Code	Number	Percentage
1	United States	US	400 000 000	9.31323%
2	China	CN	50 000 000	1.16415%
3	Japan	JP	55 000 000	1.28057%
4	United Kingdom	UK	92 000 000	2.14204%
5	Germany	DE	40 000 000	0.93132%
6	Korea, Republic of	KR	20 000 000	0.46566%
7	France	FR	20 000 000	0.46566%
8	Brazil	BR	30 000 000	0.69849%
9	Canada	CA	35 000 000	0.81491%
10	Italy	IT	7 000 000	0.16298%
11	Netherlands	NL	9 000 000	0.20955%
12	Australia	AU	19 000 000	0.44238%
13	Russian Federation	RU	30 000 000	0.69849%
14	India	IN	18 000 000	0.41910%
15	Taiwan, Province of China	TW	8 000 000	0.18626%
16	Spain	ES	8 000 000	0.18626%
17	Sweden	SE	21 000 000	0.48894%
18	Mexico	MX	13 000 000	0.30268%
19	Singapore	SG	26 000 000	0.60536%
20	South Africa	ZA	10 000 000	0.23283%

Table 4: Top 20 countries by address space propagation after lockin

9 Conclusion

The proposed project would simplify and and reorganize the process of InterNet extension and maintenance by creating coherent data source where current structure of the interconnections of ASes would be reflected as well as address space leased. This is achieved by introduction of the DLT which stores data about address space and AS neighbors. Small changes to the BGP state machine would provide mechanism to reflect link state in the DLT and would provide reliable path info for routing purposes. Reliable peering data along with prefix data would mitigate few of attack vectors including: ASes would see which prefixes could be announced by the peer. As all the address space would be reflected in the DLT the ability to announce prefixes not reachable by the AS would be easily spotable. Thus accidental InterNet disruptions would be less probable.

When the majority of AS owners would join the project and would accept unified rules it would be much easier for new participants to join InterNet as the rules would be unified and the issue with address space availability would not be as painful. The inflation mechanism in transactions would prevent squatting of address space forever. The AS fee would be equal for all AS owners. The path to join InterNet would be as straightforward as: find peers nearby and ask

them to establish BGP session, generate public key, make positive balance for it, and acquire address blocks.

References

[1] https://bitcoin.org/bitcoin.pdf

[2] https://lightning.network/lightning-network-summary.pdf

[3] https://datatracker.ietf.org/doc/html/rfc4271

[4] https://chialisp.com/

[5] https://chain.link/whitepaper

[6] https://www-public.telecom-sudparis.eu/~maigron/rir-stats/rir-delegations/world/world-asn-by-number.html

[7] https://www.imf.org/external/datamapper/PPPPC@WEO/OEMDC/ADVEC/WEOWORLD