Blockchain-based security protocol for Domain Name system client identity protection

elloh.adja@rschain.net

July 7, 2022

Table of Contents

Table of Contents

The Domain name system (DNS)

The domain name system

- is a distributed computing service used to translate Internet domain names into IP addresses or other records.
- Needed by applications to communicate on internet
- It is hierarchical and insecure

The Domain name system (DNS)

Composed by:

- DNS client
- Local DNS Server
- Resolver
- Name servers

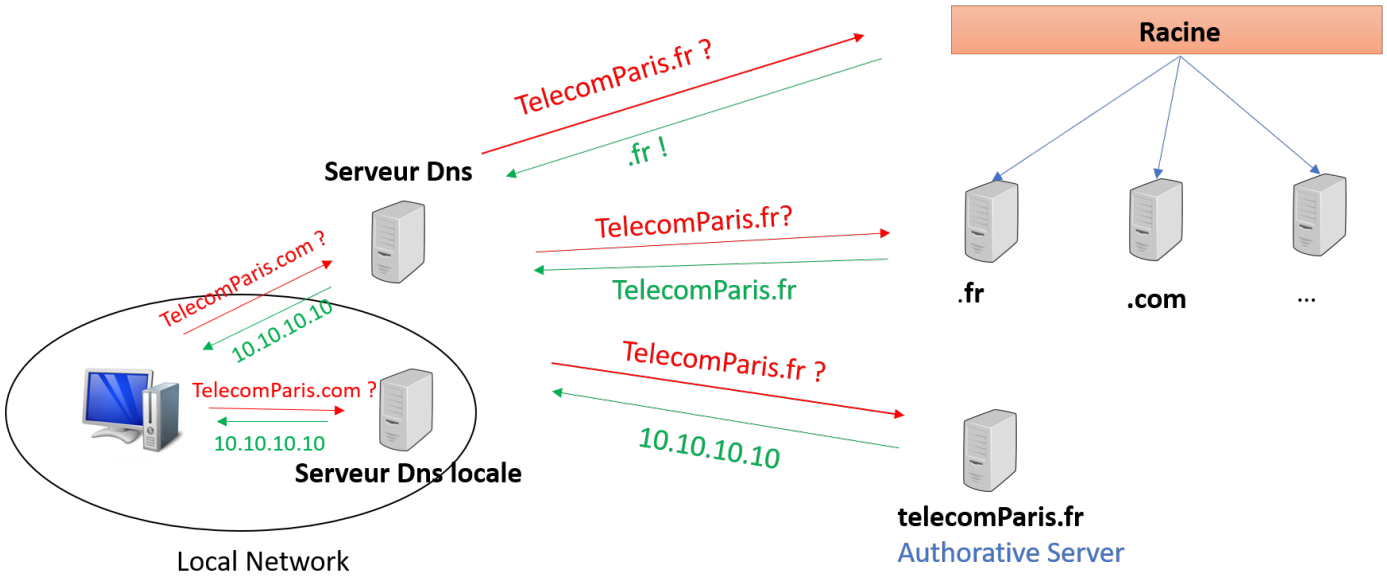


Figure: DNS request

Execution modes

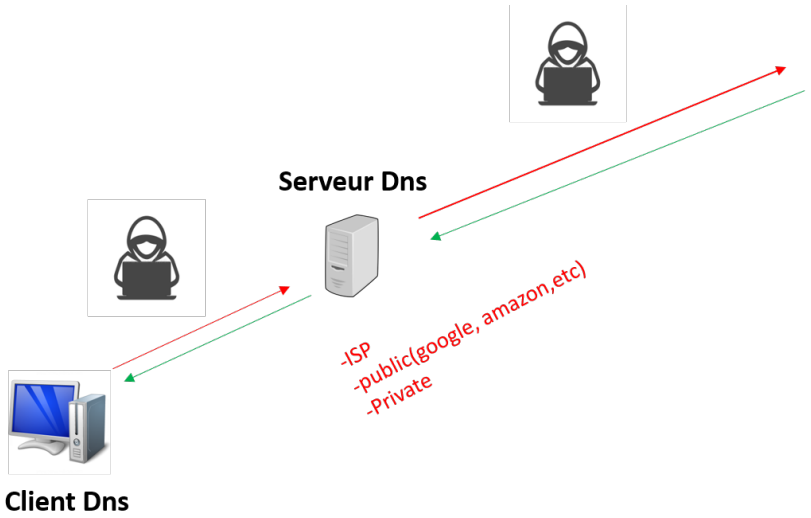
There are two execution modes:

- Recursive
- iterative

DNS security

Attacker models

- malicious user
  - for espionage purposes
  - for identity theft
- ISP or DNS server provider
  - for commercial purposes
- Government or institution
  - for censure, mass surveillance



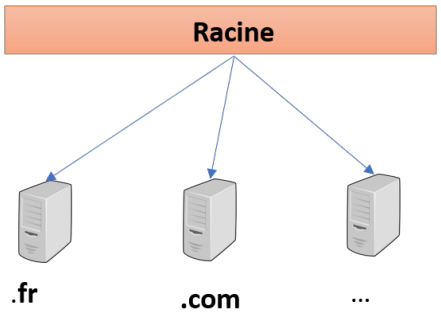


Table of Contents

Existing solutions

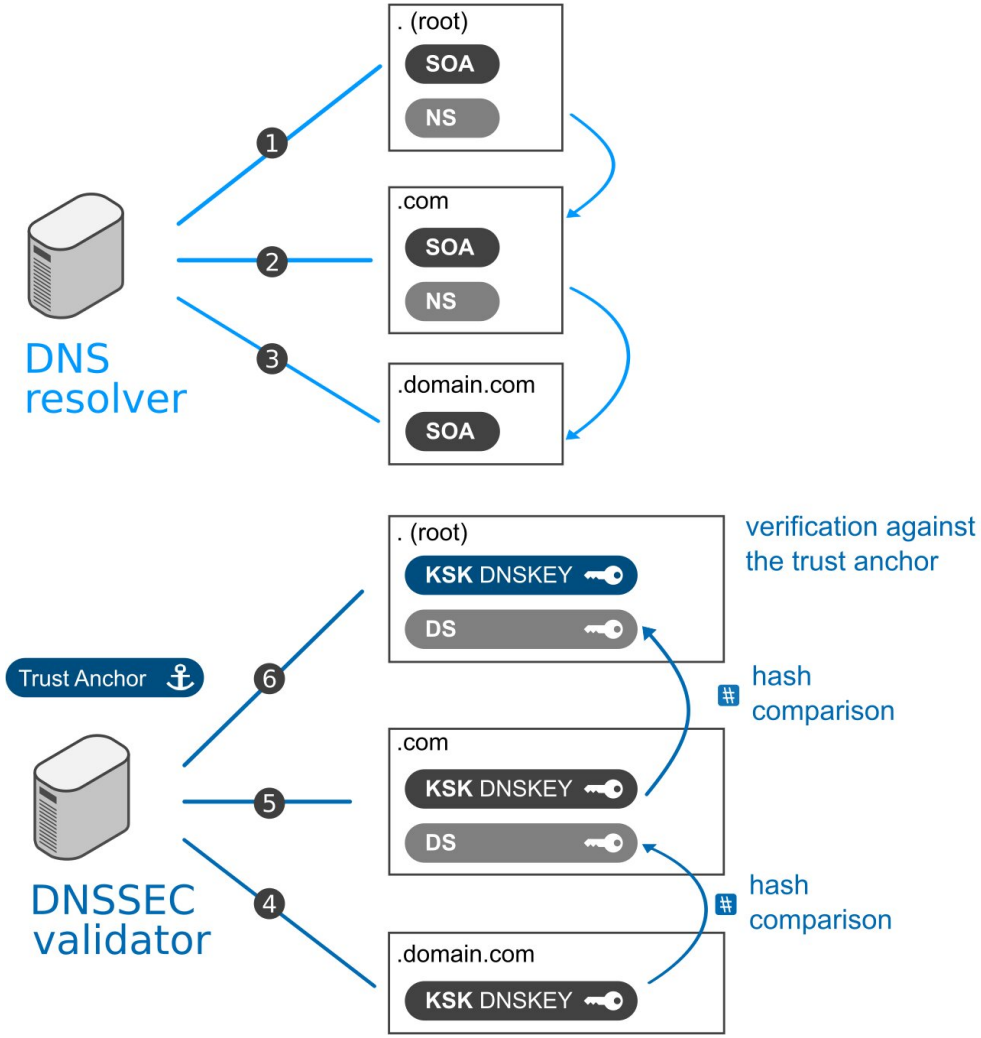
DNS security solutions:

- DNSSEC
- DNS-over-TLS (DoT)
- DNS over https (DoH)
- DNSCrypt
- DNSCurve
- Namecoin
- Blockchain namespace (BNS)

DNSSEC

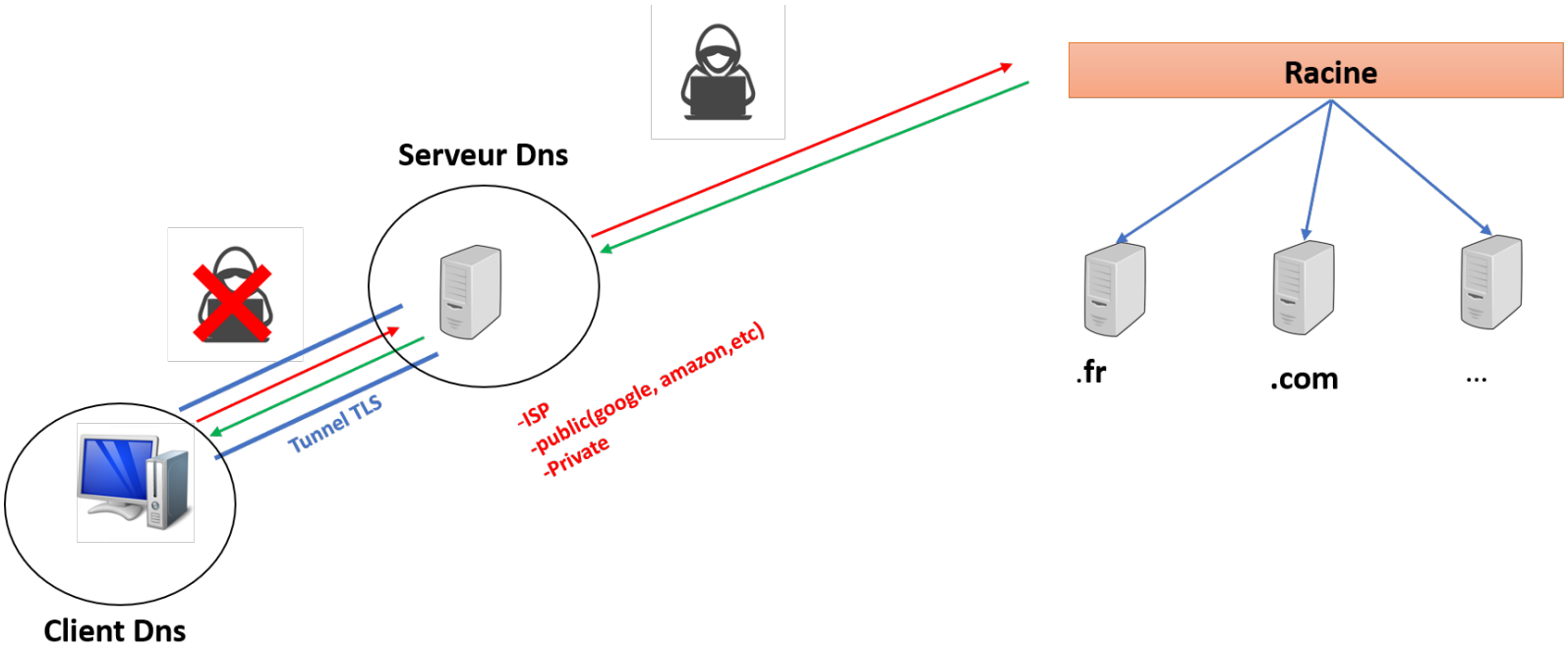
The solution is decribed by the RFC 4033

- for DNS request and DNS response authentication Cannot protect users privacy



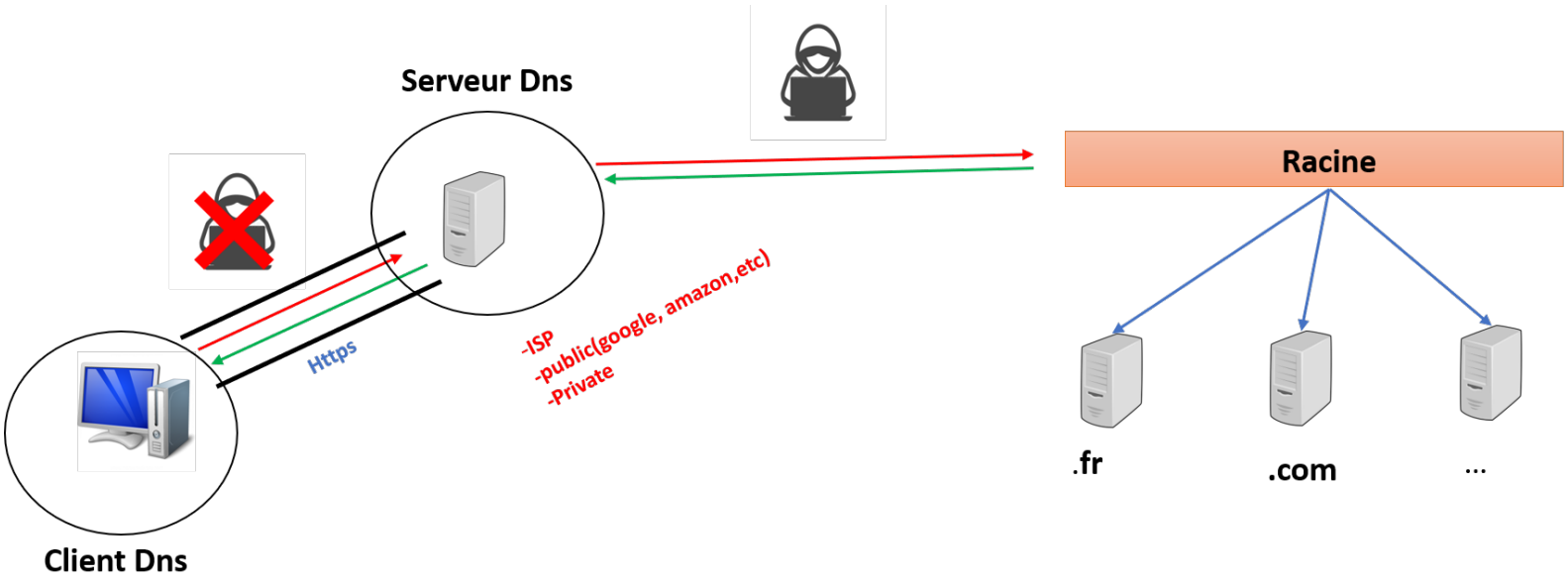
Dns-over-TLS (DoT)

- It's a standard proposed by IETF in RFC 7858
- Allows DNS queries encryption through TLS protocol
- it provide:
  - confidentiality
  - data privacy from eavesdroppers
- Cannot provide users privacy



Dns-over-HTTPS (DoH)

- It's a standard proposed by IETF in RFC 8484
- Allows DNS queries encryption through HTTPS protocol
- Cannot protect users privacy from resolvers



DNSCRYPT and DNSCURVES

- DNSCrypt
  - ensures the confidentiality of queries between the resolver and the DNS client
  - uses signature to authenticate name servers responses
- DNSCurves
  - solutions for securing DNS Protocol using 256-bit elliptic-curve cryptography
  - provide confidentiality and protection from replay attack
- Cannot protect users privacy

Oblivious DNS over HTTPS (ODoH)

Les solutions de la sécurité doivent contribuées à satisfaire les critères suivants:

- standard solution proposed by IETF For DNS security
- It is an extension to DNS Over HTTPS (DoH)
- Allows:
  - hiding client IP addresses via proxying encrypted DNS transactions
- Introduce new intermediaries servers, so more complexity

NAMECOIN

- It is a Blockchain-based cryptocurrency that realizes a decentralized namespace
- used for domain-name resolution for the '.bit' alternative TLD, and by the online identity service
- it exploit somme blockchain features to provide
  - decentralization (resistant to single point of failure)
  - Immutability
  - Anonymity
- Blockchain namespace (BNS)
  - Proposed by Blockstack as a replacement of traditional DNS
  - It binds underlying Blockchain names and cryptographic key-pairs
- It are an DNS alternative system

Solutions comparison

Criteria	Confidentiality	Auth.	Privacy	Integrity.
DNSSEC		✓		✓
DNSCRYPT	✓		✓	
DoT	✓			✓
DoH	✓			✓
BNS			✓	✓
DNSCurve	✓			✓
ODoH	✓		✓	✓
Namecoin		✓		✓

Table of Contents

Our solution B-dns

- Goal
  - New solution to secure traditional DNS system
  - Protect DNS users privacy
    - decoupling identity from the request
    - Avoiding traceability, censure and massive surveillance (ISPs, DNS servers providers, ecc.)
  - powered by a public Blockchain
    - high distribution (no single point of failure)
    - data integrity protection
    - transparency
- Attacker models
  - Attacker outside of victim network (eavedroppers)
  - The resolver of an intermediary between DNS client and nameservers

Blockchain solution constraints

- Blockchain openness
  - Public
- Anonymity
  - effective o relative
- Cost
  - transactions cost
- Blockrate
  - competitive
- Consensus algorithm
- Data capacity
- Decentralization
  - Node distribution

Stats

DNS

- Average of 120k requests/s (ICANN)
- Average of 34 queries/h by single IP address (ICANN)
- Lookup average 20-120 milliseconds (Yslow)
- Average of message size 600 octets (ICANN)

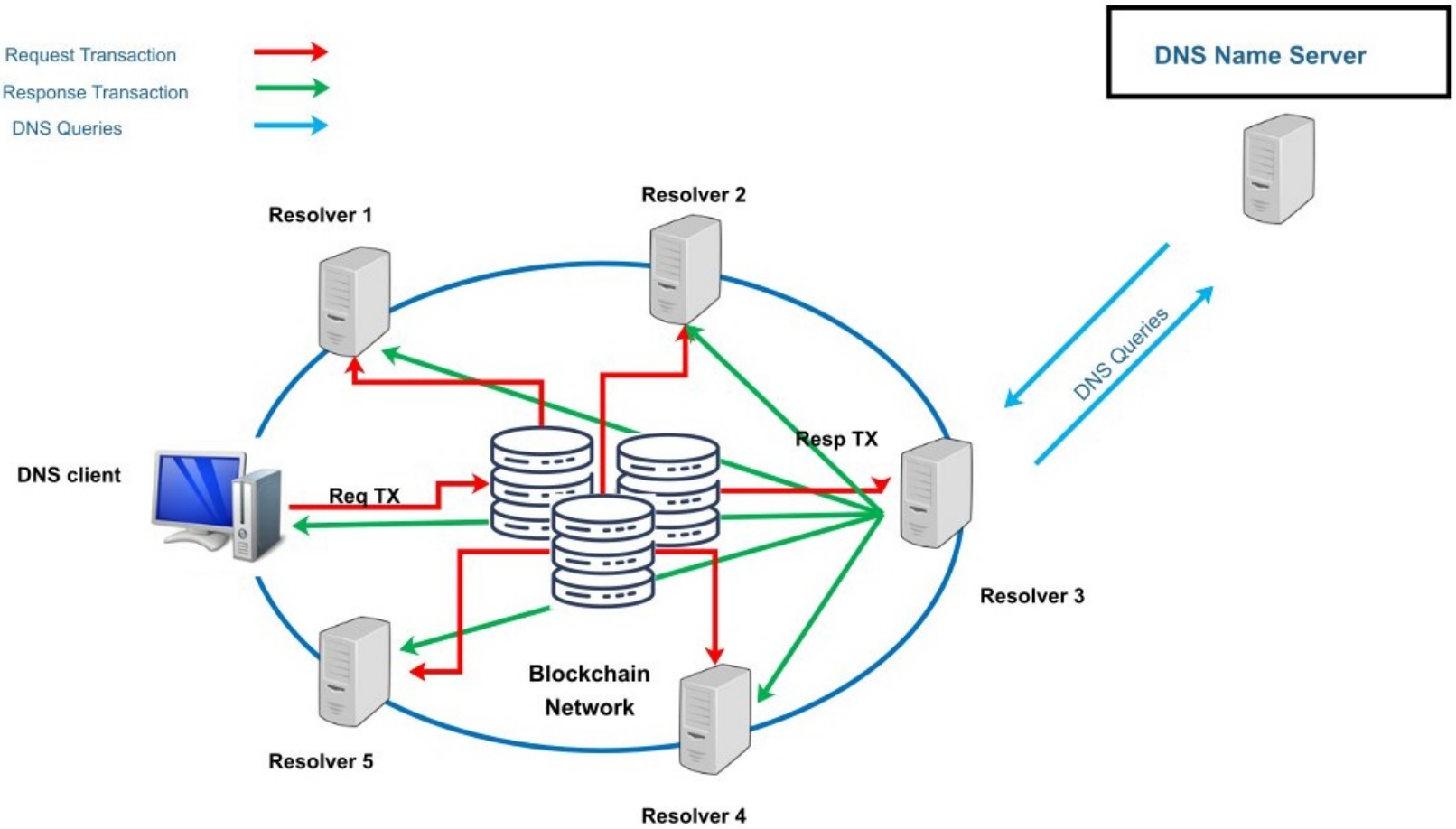
Blockchain

- TPS: 7 - 3000
- Block time /h: 6 - 6000
- Network size: 5000 - 15000 nodes

Our solution B-dns

- Attacker models
  - Attacker outside of victim network (eavedroppers)
  - The resolver of an intermediary between DNS client and nameservers
- our solution
  - Works in a recursive way
  - Use of responses cache

Our solution B-dns



Data encapsulation

- No restrictions on transaction size
- Transaction data field allow all type of data

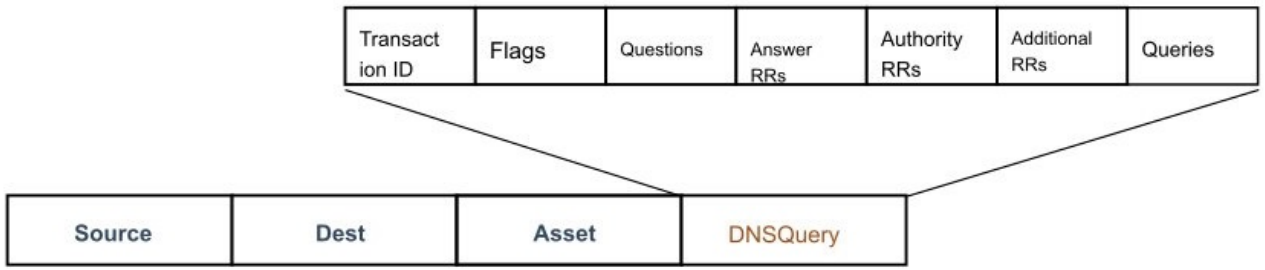


Figure: B-DNS data structure

Questions

Questions?

References I

- https://datatracker.ietf.org/doc/html/rfc4033
- https://www.internetsociety.org/deploy360/dnssec/tools/
- https://www.icann.org/resources/pages/dnssec-what-is-it-why-important-2019-03-20-fr
- https://www.infoblox.com/glossary/dns-over-tls-dot/
- https://datatracker.ietf.org/doc/html/rfc7858
- Deep Packet Inspection, Jens Myrup Pedersen, Aalborg University
- https://www.akamai.com/fr/our-thinking/cdn/what-is-a-cdn
- https://www.avast.com/fr-fr/c-what-is-a-vpn