BitRezus

Blockchain in the telecommunication industry

Conceptually a new effective solution to prevent fraud on the networks of Communications Service Providers and reducing operational costs.

Application scenarios

The use of private blockchain based products to build telecommunication infrastructure.

Mobile number portability MNP

The use of subscriber profiles in a distributed storage network to provide the MSISDN number portability function from one PLMN mobile operator to another.

Roaming subscribers

Distributed data storage of subscriber profiles between roaming partners.
Use in a distributed network of data storage as a single database of subscribers - operators of roaming partners for reduction.

Revenue Assurance - Call Data Records

Storage of all information about the rendered roaming services for subscribers in a single decentralized CDR database available for the roaming partner excluding the possibility of manipulation, loss and change of data usage to ensure guaranteed income for provided communication services.

IoT - Distributed Digital Ledger

Ensuring P2P interaction between devices, creating a database of profiles for hundreds of millions devices and submitting this data to customers

Attention - Fraud!
$ 0.5-1.5 per subscriber

According to the Communications Fraud Control Association report for 2017, the main methods of fraud related to the use of voice services are:

- $ 3.67 billion - fraud with authorization (user identification) and interception of accounts
- $ 4.27 billion - bypass interconnection (SIM box)

Identification data of subscribers, which fraudsters use for enrichment, are considered as the most vulnerable. This most often occurs at the moment of user authentication in roaming networks.

Types of fraud

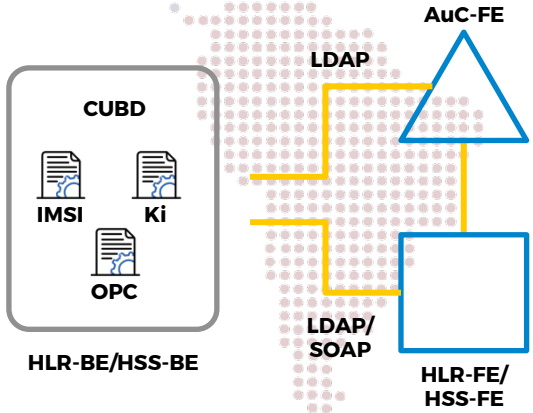
Main manipulations using subscriber identity data:

- Using subscriber data to access services
- Subscriber accounts management for services (resale)
- Using SIM boxes with cloned subscriber data to bypass traffic origination and interconnections

BitRezus

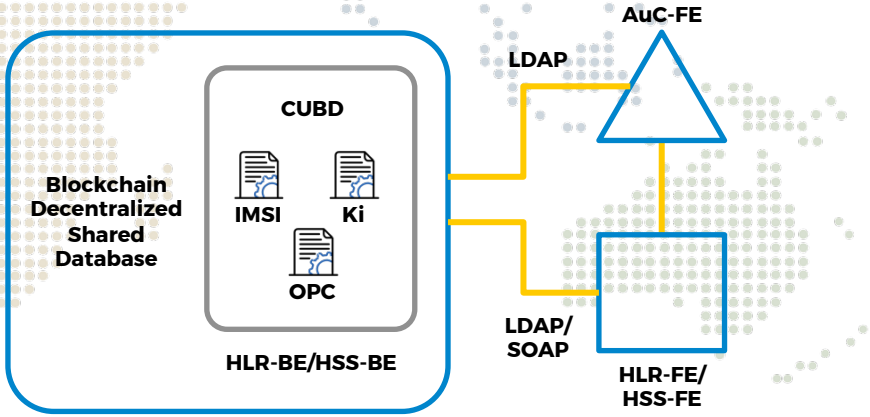
Traditional HLR/HSS

Each operator implements a separate database for profile storage and the entire exchange takes place over public signaling networks, messages in which may be subject to delay, interception, modification and cloning.



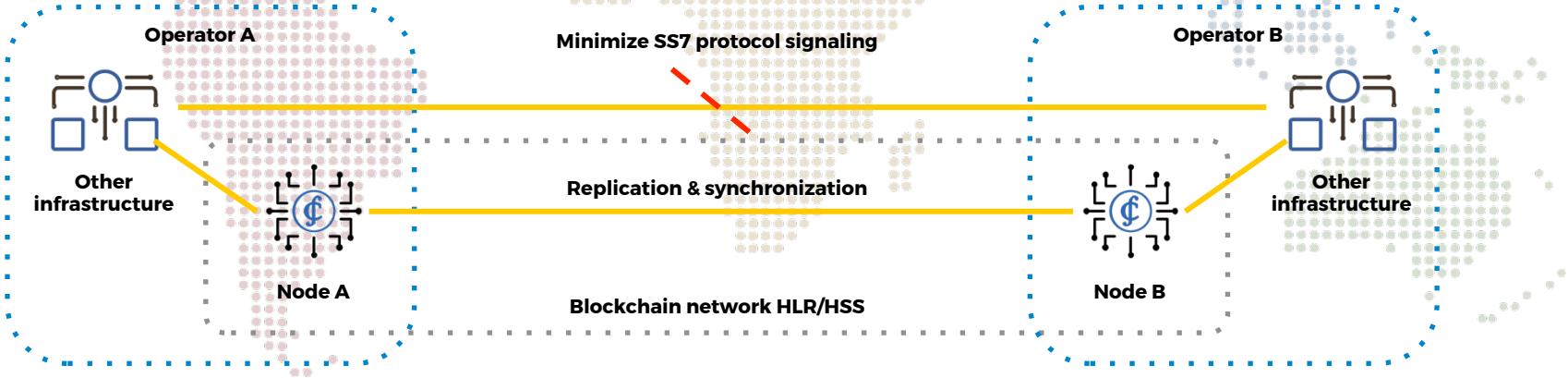
Decentralized HLR/HSS

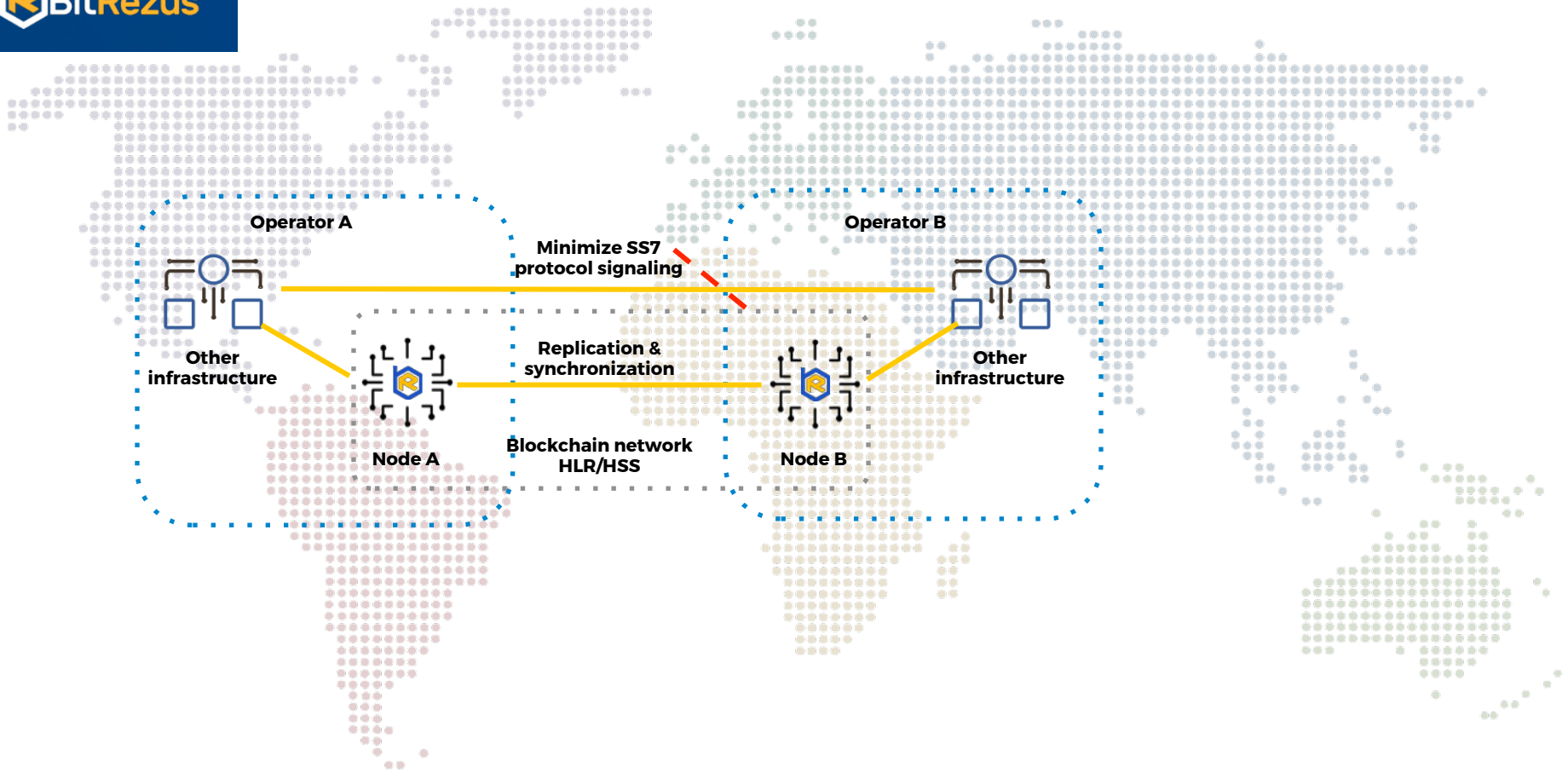
We propose to implement a decentralized HSS using the private blockchain between roaming partners to instantly exchange encrypted authentication keys.



Roaming interaction

We propose to implement a decentralized HSS using the private blockchain between roaming partners for instant exchange of subscriber profiles, due to the fact that the Operator will apply to a single database of subscriber profiles that is faster and more reliable.




Operator A
Minimize SS7
protocol signaling
Operator B
Other
infrastructure
Replication &
synchronization
Other
infrastructure
Node A
Blockchain network
HLR/HSS
Node B

Implementation scheme

We propose a new HLR / HSS architecture, in which we retain all the functionality of HLR-FE, HSS-FE, AuC-FE providing integration with all mobile network nodes (MCS / VLR, MME of home network and roaming partner network), while we transform HLR-BE, HSS-BE classic centralized subscriber database (e.g. Ericsson CUDB) to a decentralized private blockchain network solution with at least a couple of nodes (one in a home network and one in a roaming partner).

These nodes will support the same interfaces to interact with the HLR-FE, HSS-FE, AuC-FE subsystems, specifically LDAP / SOAP, and the main function of secret subscriber identification parameters storage (IMSI, Ki, OPC, etc.) and the classic centralized HLR / HSS database. But the parameters requested during authentication and triplet generation process (RAND, Kc, SRES) by the authentication center AuC-FE (IMSI, Ki, OPC) will not be transferred from the centralized HLR / HSS database, but from the local node of the private blockchain network.

Thus, the validation of the transmitted parameters for each authentication procedure (Location Update) of the subscriber, both in the HPLMN home network and in the VPLMN roaming partner network, is performed by both operators.

Credits blockchain solutions advantages

Partner operators agree on joint encrypted storage of partial information from subscriber databases and authentication keys in the blockchain network deployed on the basis of the private blockchain.

A single database of constantly synchronized data allows you to reduce the amount of data transmitted during SS7 roaming and reduces the operational costs of roaming partners without violating the requirements of 3GPP standards.

This will allow the authorization of subscribers in real-time, which completely eliminates subscription fraud and the use of SIM boxes to bypass interconnections.

This solution minimizes the costs for operators to combat general methods of fraud, strengthens trust relationships between roaming partners and allows creation of a protected ecosystem.

Why to choose BitRezus?

We have created a unique blockchain ecosystem, which allows you to use blockchain technology stack in every industry

- Unified protocol of release, storage, transfer of financial assets
- Infrastructure in the form of a distributed network with a public registry
- System accounts with public and private keys
- Set of security systems
- Built-in programming language for creating services

Contact us

We have a team of strong programmers and Technology Consultants who can Help you with the PoC (proof of concept) and MVP

Visit our website : https://bitrezus.com