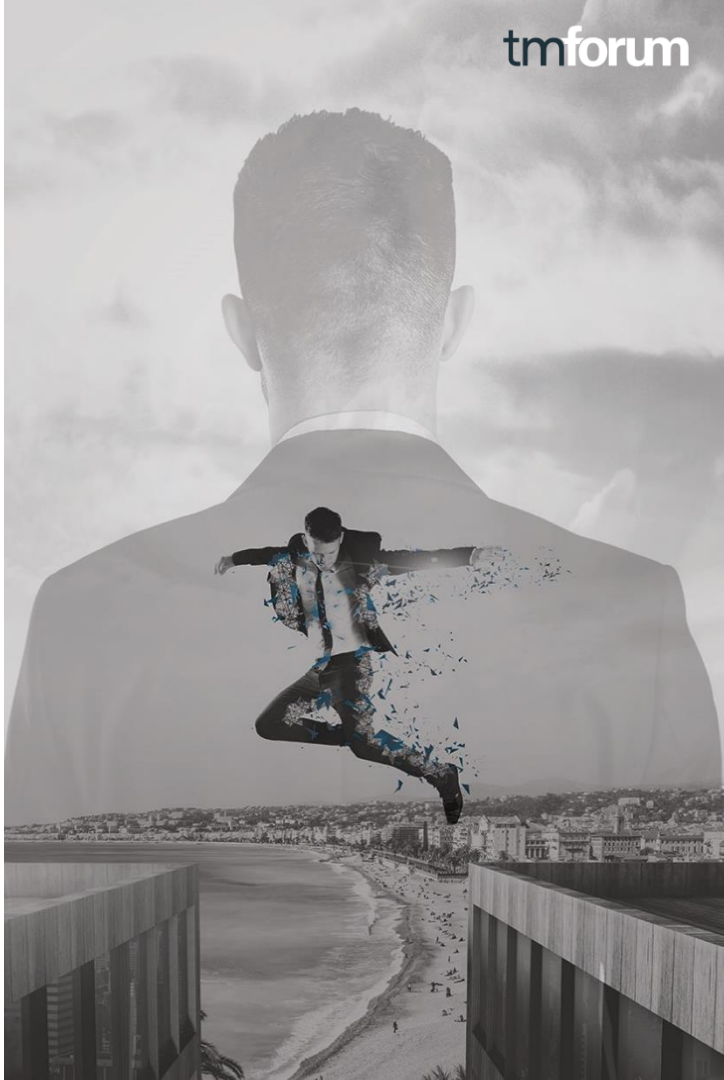
Blockchain Unleashed



Contents

- Introduction
  - Catalyst team
  - Blockchain for CSPs
  - Criteria for use case section
  - Use case scenarios
- Use cases for blockchain in CSPs
  - Use case 1: Elimination of CDRs - Roaming
  - Use case 2: Identity Management
  - Use case 3: SLA Monitoring
  - Use case 4: Prevention of Phone Theft
  - Use case 5: Mobile Number Portability
- Key learnings

Introduction

Catalyst Project Team

tmforum

Champions

BT

Globe

KDDI

KDDI Research

OPTUS

orange™

Singtel

Telefónica

ultrafast FIBRE

vodafone

Participants

Deloitte.

IBM

Infosys

OPENET

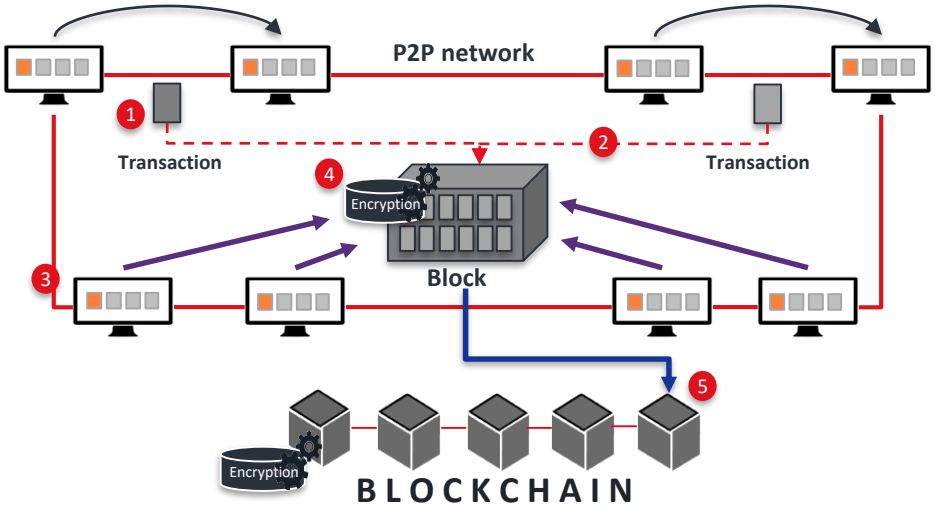
Blockchain technology can be truly disruptive to CSPs outside of the FinTech industry.

The premise of blockchain seeks to eliminate the use of middle-men entities in certain operating models resulting in reduced cost of operations and can generate new revenue streams through new services provided by CSPs.

What is blockchain?

A blockchain is a distributed ledger technology which allows any participant in the business network to see the system of record (ledger).

The most popular application of blockchain technology is Bitcoin based on payments, however new applications are being developed with uses across multiple industry outside of payments.



How does a blockchain work?

1. Interaction of computers generate individual, unique **transactions.**
2. Transactions stored chronologically in **blocks**.
3. Nodes (computers in the blockchain) validate the block of transactions to form a **consensus**, which ensure data integrity in the blockchain.
4. Once the block reaches a level of validation, it's **cryptographically** secured.
5. The block is cryptographically linked with the other blocks as the latest entry, thus forming a **chain**. Succeeding transactions are placed in a new block.
6. As new blocks enter the blockchain, it is replicated across all computers connected to the network.

Criteria for use case selection

Each use case was reviewed on the below criteria for consideration to the Blockchain Catalyst

- There's a need to share information.
- There's a need for multiple organizations/departments to have write access to the information.
- There's a need for a complete and transparent historical record.
- There's a good reason to eliminate intermediaries.
  - Lowering cost, faster and/or automated consolidation of data, or the inability to have a trusted intermediary.
- There are interactions between the transactions.
  - Smart contracts come into effect when transactions depend on one another.

- Use cases may or may not fulfill all 5 conditions, as long as those fulfilled conditions maximize the benefits of using blockchain.
- Ultimately, these points serve as a guide to avoid using blockchain just for the sake of using it.

Sources: STL, TMForum

Use case scenarios

Five use cases selected for the Blockchain Catalyst

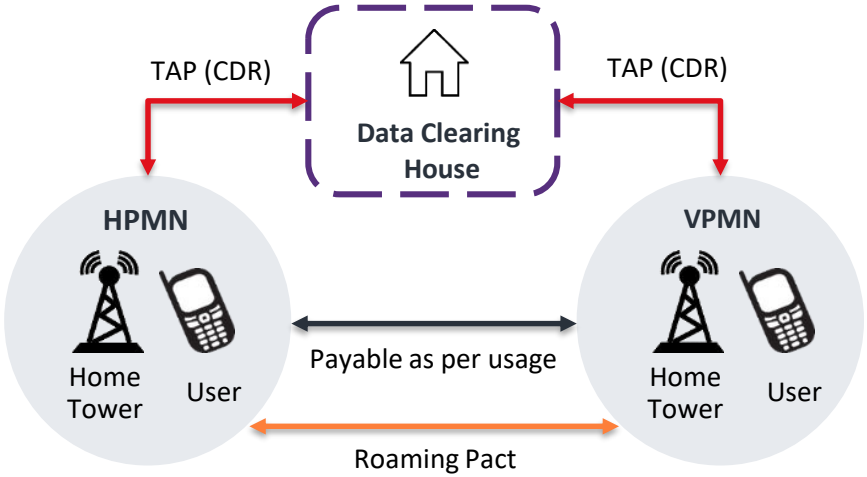
1. **Elimination of Call Detail Records (CDRs)**
2. **Identity Management**
3. **Service-Level Agreement (SLA) Monitoring**
4. **Reducing Mobile Phone Thefts**
5. **Mobile Number Portability**

Use case 1:
Elimination of CDRs for Billing, Settlement, Fraud Detection.

Current state process and challenges

Current process

- When a call is placed, the **Visiting Public Mobile Network (VPMN)** queries **Home Location Register (HLR)** of **Home Public Mobile Network (HPMN)** to find about users subscribed services.
- As per availability or schedule, say multiple time a day or week (as per bilateral agreement), **VPMN sends a TAP file (with the CDR) to HPMN** via **Data Clearing House** which is responsible for transmission and conversion of TAP file.
- HPMN must **settle accounts per costs** incurred with the VPMN in accordance with the roaming agreement tariffs (account settlement between Roaming partner based as inter operator tariff (IOT).



Challenges

Costs incurred of fraudulent subscribers, resulting in inaccurate billing

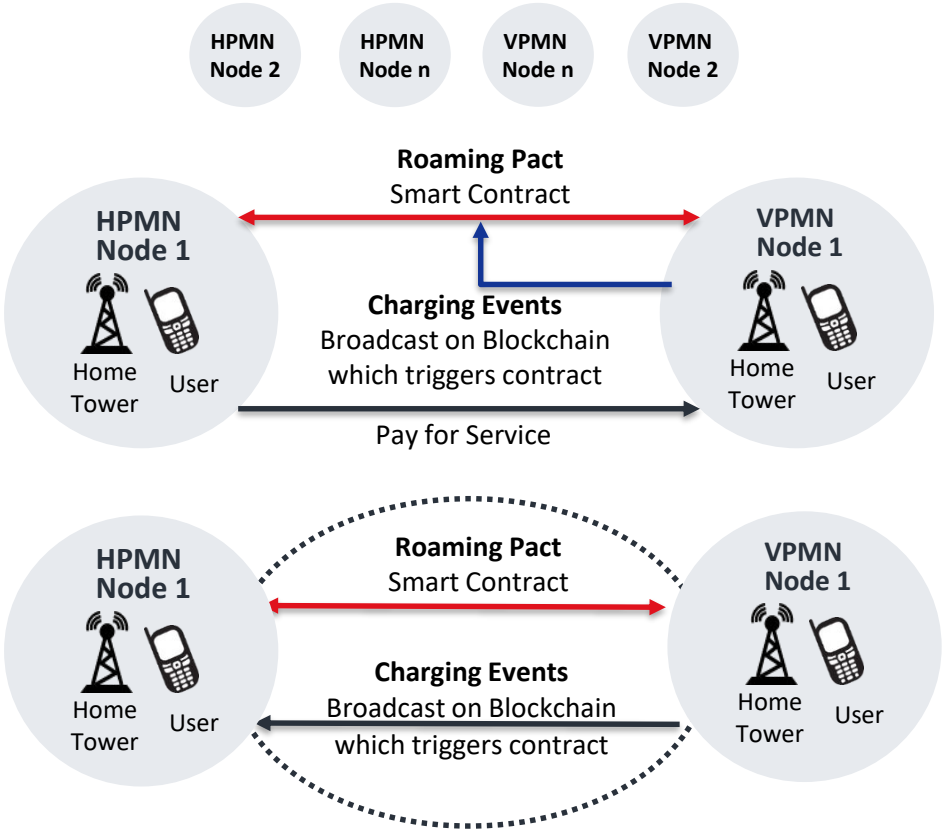
- When a **fraudulent subscriber uses home network resources** via the partner network but the home network can't charge the subscriber. The **home network still has to pay** the partner network for roaming services.

Time required to detect fraud results in longer settlement

- Fraud occurs when the subscriber is not within the home network. The **time required to detect fraud** is **extended** due to **delays in the exchange of data** between the home network and partner network.
- Since the fraud occurs outside of the home network, it takes a **longer time** to respond to it.

Eliminating CDRs: Blockchain solution architecture

Overview of Blockchain Network



Benefits:

Near **real time data** availability to all participants in the network resulting in:

- Fast action on roaming data provided.
- Automatic triggering of roaming contract enables near-real-time charging which reduces roaming fraud.

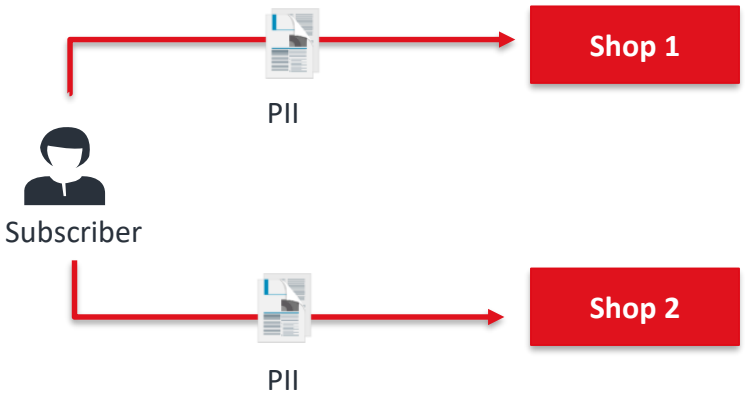
- Faster dispute resolutions through clear transaction history between operators.
- **Single source of truth** is maintained to reduce multiple conversations between parties hence reducing disputes.
- **Cost savings** from removing the data clearing house.

Use case 2:
Identity Management

Current state process and challenges

Current Identity Management process

- For every service a subscriber wants to use, it is required to **register** and **create an ID with each vendor**.
- This requires each vendor to **validate** and store the subscriber ID, resulting in **different customer PII information** and customer usernames/passwords across vendors.



Challenges

Data security

- Personal Identity Information (PII) is stored across different websites/applications or different subsidiaries. This can result in:
  - Potential data hacks.
  - Exploitation of PII by third-party entities.
  - Multiple login usernames and passwords which are are difficult to maintain and easily forgotten by users.
- Passwords and PINs are increasing becoming an unsafe mechanism for authentication.
- Printed PII is easily lost and difficult to replace, for example, ID and debit/credit cards.

Verification processes

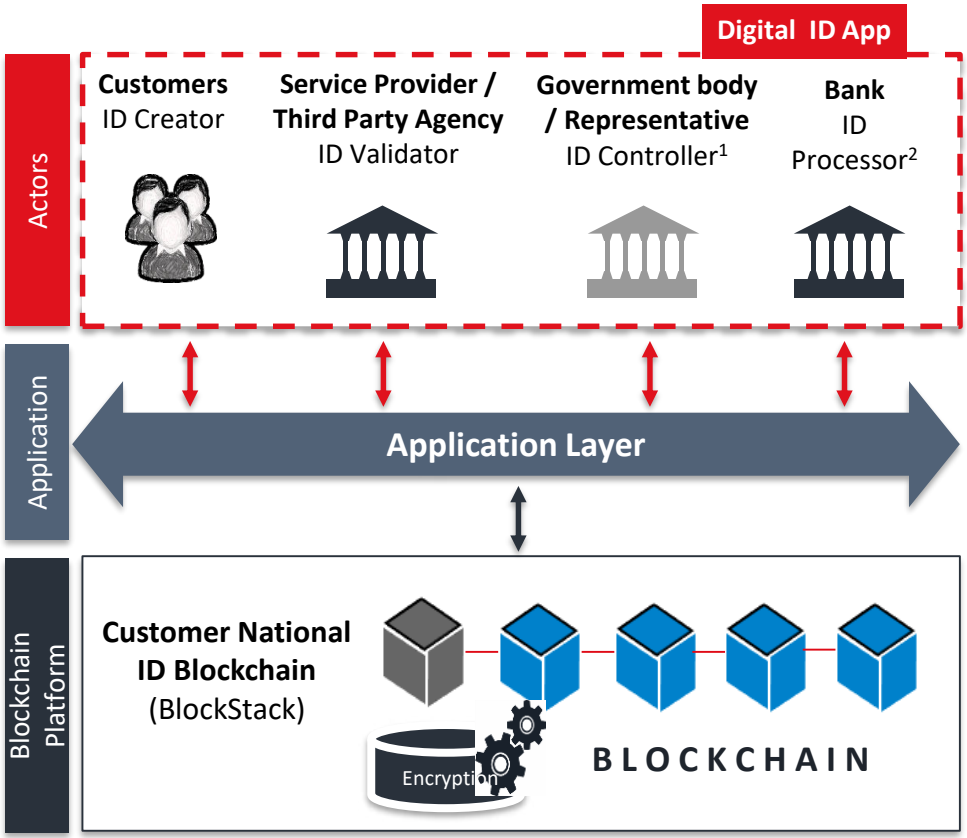
- Manual verification of PII is time consuming.
- Integrity of shared information to website/application can be questionable.

Customer experience

- Lack of convenience due to multiple user names and passwords.
- Customers hesitant to use third party Single Sign On (SSO) for accessing new vendors.

Identity Management: Blockchain solution architecture

Overview of blockchain



[1]Goverment body / representative that provides IDaaS platform. [2]Third party enterprises that requires verified ID details

Benefits:

Only **one digital ID** is maintained on the blockchain giving single source of truth

- **Know Your Customer (KYC) data** including address proof, ID proof, photo and other information can be mapped with the blockchain ID.
- Ease of business and improved overall **customer experience.**
- Cost savings from using a blockchain solution compared to a traditional Identity management solution.
- New revenue stream by offering Identity Management as a service (IDaaS) solution to partners and consumers.

Use case 3:
SLA Monitoring

SLA Monitoring: Current state process and challenges

Current SLA monitoring process

1. Customer will log incident to Telecom, for example, Globe.
2. Telecom will create an incident ticket and assign to internal investigation group.
3. Investigation group after investigation will respond that external vendor support is needed.
4. Globe, service provider will create vendor task and send to vendor via email.
5. Vendor will accept and allocate task.
6. Vendor will troubleshoot and update task.
7. Vendor will close ticket and notify Service provider via email.
8. Globe, service provider will update ticket and confirm resolution with customer.
9. Customer will verify closure.

Challenges of existing SLA monitoring

Manual processes resulting in errors and delays in processing SLAs

- SLAs need to be **manually reviewed** and **corrected**.
- **Delays in processing response** from vendors due to manual processes requiring email and phone not automated.

Disputes between vendors resulting in delays in payments

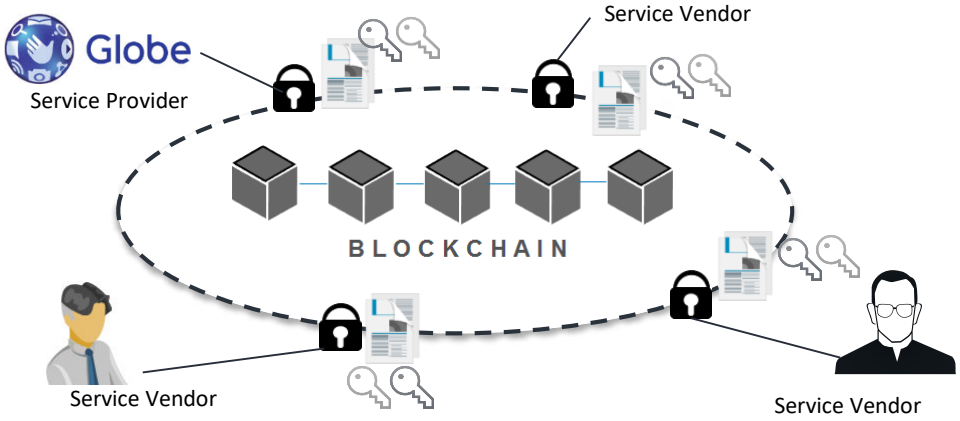
- SLAs from contracts need to be **manually interpreted**, potentially resulting in **different interpretations** by vendors and service providers, causing **disputes**.

SLA ticketing system relies on manual ticket creation

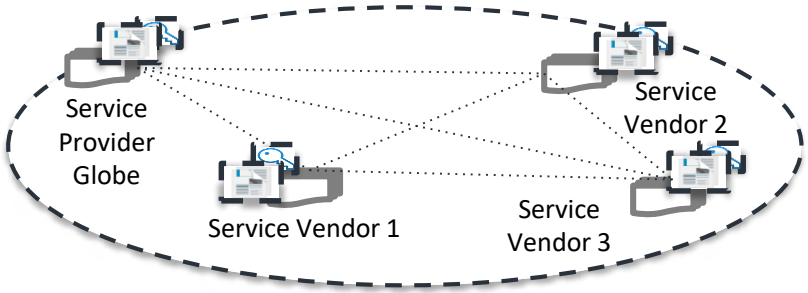
- Emails to create/update tickets may **not be reliable**, can cause **duplicate tickets** created.
- Full API ticket integration between service provider and vendor can be **costly**.

SLA Monitoring: Blockchain solution

Overview of blockchain for SLA monitoring



Blockchain node representation of service provider and vendor



Benefits:

Real time transparency of **data** on the network in addition to the SLA on the blockchain as one source of truth resulting in:

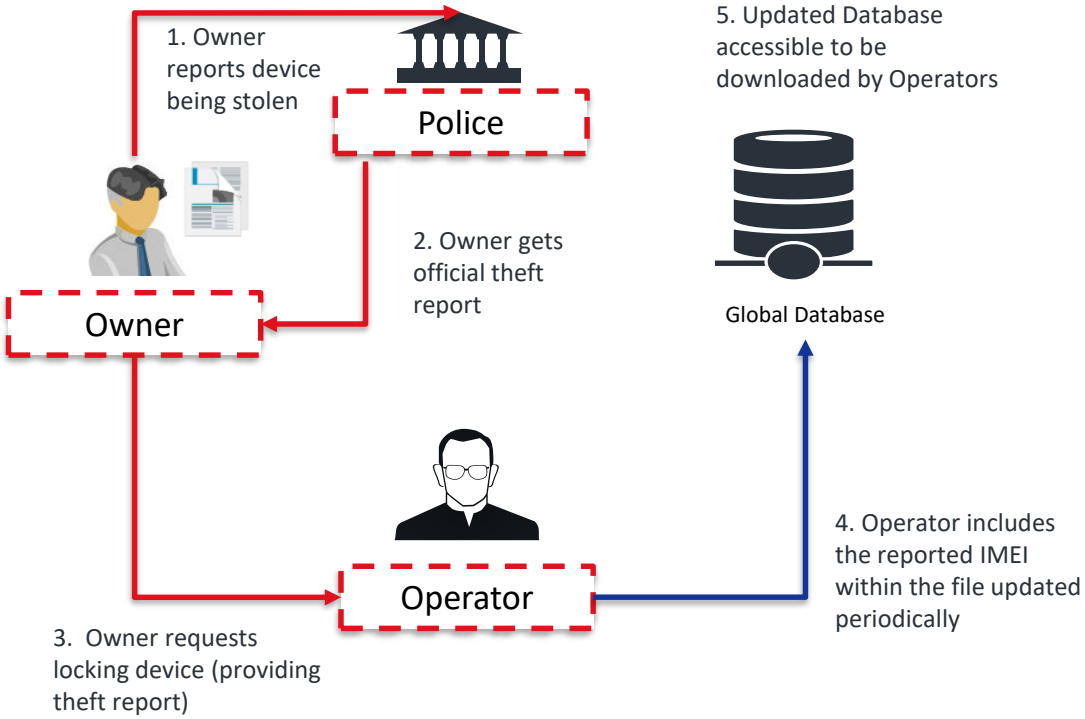
- Real time settlement and visibility.
- Vendor and Service provider see same SLAs.
- Reduced number of disputes between Vendors and Service Providers as both have full visibility of SLAs

- **Reduced settlement times** due to:
  - Vendor engaged faster through blockchain.
  - Updated SLA on closure is instantaneous.
  - SLAs automatically calculated.
- Significant **reduction in the cost** of SLA monitoring due to reduced time to implement and manage SLAs.

Use case 4:
Prevention of Phone Theft

Reducing Mobile Phone Thefts: Current state process and challenges

Current process based on a Global Database, for example GSMA.



Challenges

Manual processes resulting in errors and delays

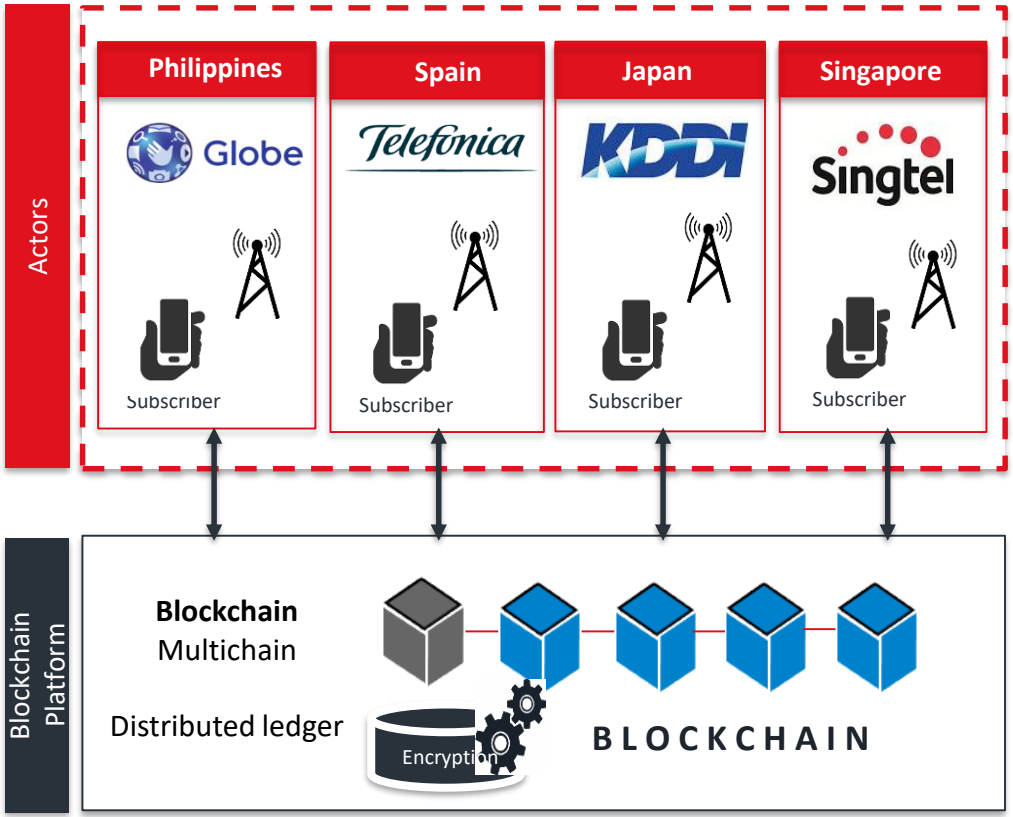
- The blocking of a device is **not instantaneous** and can only be performed by the owner´s Operator.
- Update of the Global Database is based on files **sent periodically** (**daily**) by the owner´s Operator to Global Database, for example, GSMA.

Solution is reliant on consistent operator Global Database across operators

- Blocking in a given country is guaranteed only if the Operator has **downloaded the latest updated Global Database**, for example, from GSMA.

Reducing Mobile Phone Thefts: Blockchain solution

Overview of blockchain



Benefits:

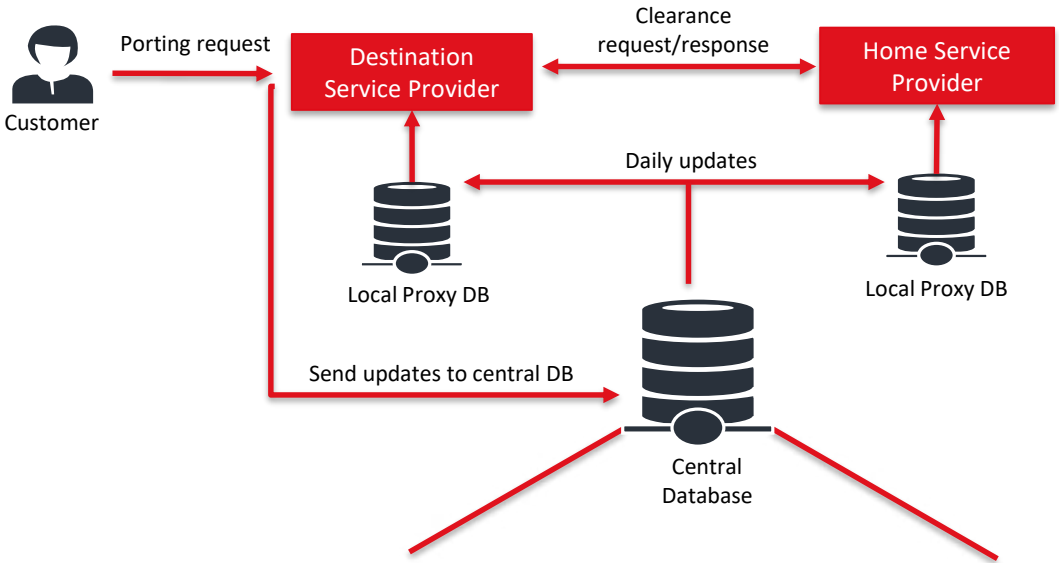
Immediate blocking of a reported stolen device within the blockchain.

- Multiple agents connected to the blockchain able to **report stolen devices** for blocking.
- Agents different than owners operator (provided authorization to update the chain) can **block a device**.
- **Smart contracts** allows third parties to be instantaneously informed of any change of status of a device.

Use case 5:
Mobile Number Portability

Mobile Number Portability: Current state process and challenges

Current process



Home Service Provider	Destination Service Provider	Mobile number
PLDT	Globe	123456…
Vodafone	Globe	456745….
…..	…..	…..

Challenges

Manual processes resulting in errors and delays

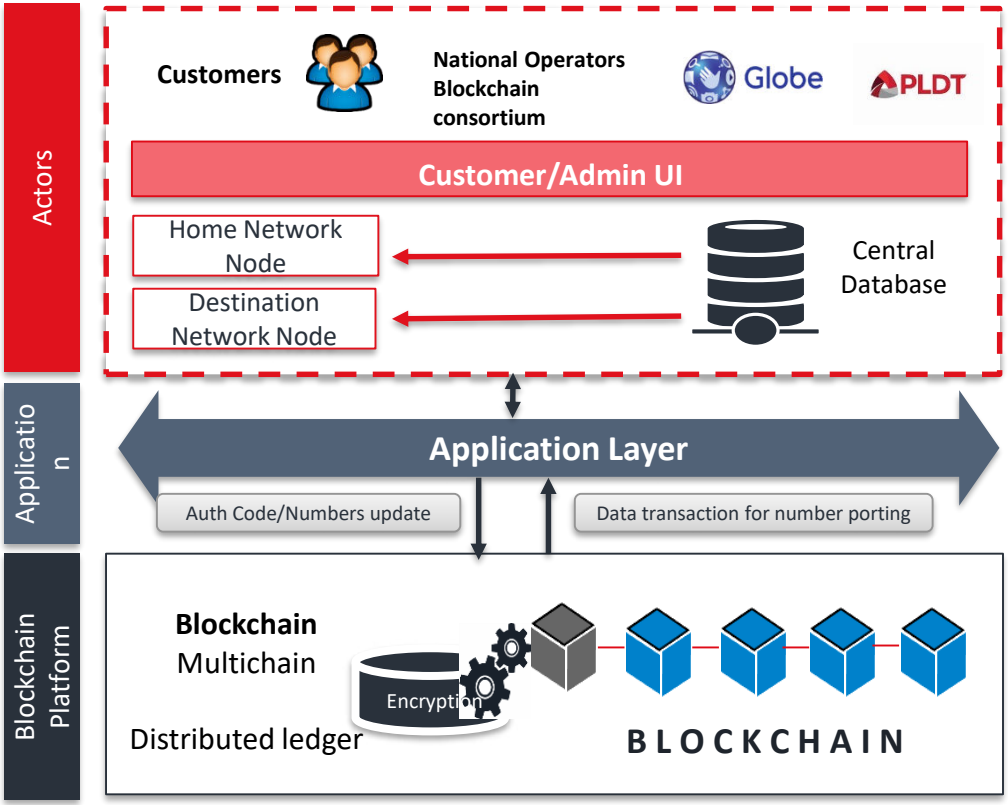
- Requests are rejected due to data mismatch between operators
- High processing time in some countries

Solution is reliant on consistent operator Global Database across operators

- Single point of failure due to central database of portable numbers
- Delays in process due to updates required of the local database from the central database periodically.

Mobile Number Portability: Blockchain solution

Overview of blockchain architecture using Multichain



Benefits:

Real time transparency of **data** and immutable data with single source of truth on the network.

- Distributed ledger would eliminate the possibility of **single point failure** as all service providers have access to the same data.
- Eliminate the delays in the process as real time view is provided by blockchain.
- **Frequent updates** of local database from central database no longer required
- All participants in the blockchain have access to the latest records.
- Hassle-free operations in order to maintain portability record.

Note: MNP process differs from country to country, based on the rules and regulations of the country regulator. Above use case detailing is based on the MNP process in India.

Key learnings

Key Learnings

1. Based on the use case context, right blockchain technology needs to chosen. E.g., for computational logic, select blockchain platforms that supports Smart Contracts like Hyperledger; for registries scenario, multichain can be efficiently used

2. Different blockchain technology has different processing capabilities, we have to be careful when determining what processes and data should be placed in the blockchain, and select right technology platform

3. There is a need to have **programmable blockchain**, to incorporate digital rules and logic from legal documents as Smart Contracts in the blockchain platform

© 2018 TM Forum | 25