

Global Market Place for Mobile Operators and Service Providers

Section 1 Summary

Use Case Summary			
Use Case ID:	ICT-001	Use Case Type:	Vertical
Submission Date:	October 11, 2018	Is Use Case supporting SDGs	No
Use Case Title:	Global market place for mobile operators and service providers	Domain:	IT & Telco
Status of Case	PoC	Sub-Domain	Mobile roaming Digital Services
Contact information of person submitting/ managing the use-case	Full Name: Alexander Yakovenko Job Title: Project Director E-mail address: ayakovenko@clementvale.com Telephone number: +7-985-991-2048 Social media: https://www.linkedin.com/in/alexander-yakovenko Web site: https://www.blockchaintele.com		
Proposing Organization	Clementvale Baltic OU, Estonia		
Short Description	This use case is a proposal to create global market place for mobile operators and service providers with the use of private Blockchain ecosystem by changing traditional roaming rules and creating new sales channels, using a stable coin for immediate payments.		
Long description	This use case is a proposal to create global market place for mobile operators and service providers with the use of private Blockchain ecosystem. The main goal is to enable mobile operators and service providers to interact directly and securely without any agreements, intermediators and complex integration via smart contracts. This solution significantly simplifies all processes, eliminates old-fashioned roaming technology, shifts principles of interaction, reduces costs on all levels, gives an easy and quick access to global market for all players in a short period of time with almost zero investment, gives a good opportunity for mobile subscribers to use services at reasonable rates worldwide, changes principles of settlements, making them in real time in stable coin. We created one of the stable token that equals 1 SDR used in telecommunications, which is tied to the basket of five world currencies. We named it SDRt (SDR Token). It's the unit of payment given to providers for their services, i.e., the price of services is measured in these units.		

SDG in Focus (when applicable)			
Value Transfer:	SDR tokens representing fiat money	Number of Users:	100+
Types of Users:	Any MNO/MVNO and/or service provider, mobile subscribers		
Stakeholders	Any MNO/MVNO and/or service provider		
Data:	Offers on mobile and non-telecom services published by operators and service providers, Requests on services, User ID, Service provider's digital code, SDR tokens flow, Other transactions related to rendering services		
Identification:	Nodes verify all transactions via consensus algorithm		
Predicted Outcomes:	<ul style="list-style-type: none"> - Elimination of any agreements, intermediators and complex integration - Change of traditional roaming rules - Reduction of mobile services costs - Secure and direct interaction between mobile operators or operators and service providers via smart contracts - Quick access to global market for small and medium-sized mobile operators and service providers - Provision of own subscribers with local rates around the world in a short period of time with almost zero investments - New sales channels for service providers 		

Overview of the Business Problem or Opportunity
<p>Current problems:</p> <ul style="list-style-type: none"> • Long and complicated process to implement mobile services in roaming, requiring negotiation between operators, signing a lot of roaming agreements, physical interconnection of networks, different tests and other integration processes; • High rates for mobile subscribers in roaming, which increase cost of this service and cause big inconvenience for end users; • Low consumption of services, which effects on decreasing of mobile operator's revenue due to huge amount of "silent roamers"; • Huge expenditures on infrastructure support; • Necessity for mobile operators to have a large staff to maintain commercial, legal and technical processes of mobile roaming services; • Marketing expenditures for service providers to promote their services <p>Blockchain technology is a platform to construct a global trusted marketplace, where mobile operators and service providers can interact directly with each other without agreements, intermediators and costly integration.</p> <p>Opportunities:</p>

For mobile operators:

- Simple and low-cost access to global roaming market.
- Provision of own mobile services to subscribers of other operators worldwide.
- Possibility to resell mobile and non-telecom services from global providers to own subscribers.

For service providers (content providers, software vendors, insurance, transportation, etc):

- New sales channels to subscribers of mobile operators.

For subscribers:

- To get high quality mobile and non-telecom services worldwide at affordable prices.

For all participants:

- Elimination of intermediators in sales chains.
- Reduced time and costs for mutual settlements between participants.
- Significantly reduced costs on technical, legal and commercial levels

Why Distributed Ledger Technology?

- Community-controlled DLT system ensures participants that the system operates according to the strictly defined software-driving rules.
- Unlike classical centralized approach, there is no party or organization that could change rules on its own. Therefore, there are minimal risks for participants and their investments.
- Minimal investments into hardware and software infrastructure.
- Exceptional reliability of the system because of inherent security, redundancy and self-restoring capability of DLT platform.

Section 2 Current process

Current Solutions

Current roaming technology is cumbersome, expensive and hard to implement as it requires a long process, including negotiations between mobile operators, approval of business cases, commitments, legal confirmation, signing hundreds of roaming agreements with each operator in each country, necessity to be a GSMA member, interconnection of networks, technical tests on different levels, proper equipment and other integration processes. It bears cost on the integration of carriers, measured in years and millions of dollars. As a result, the roaming services market has become virtually monopolized by the major carriers, and it is closed to regional carriers. The latter actually lose their subscribers at a time when they are traveling abroad.

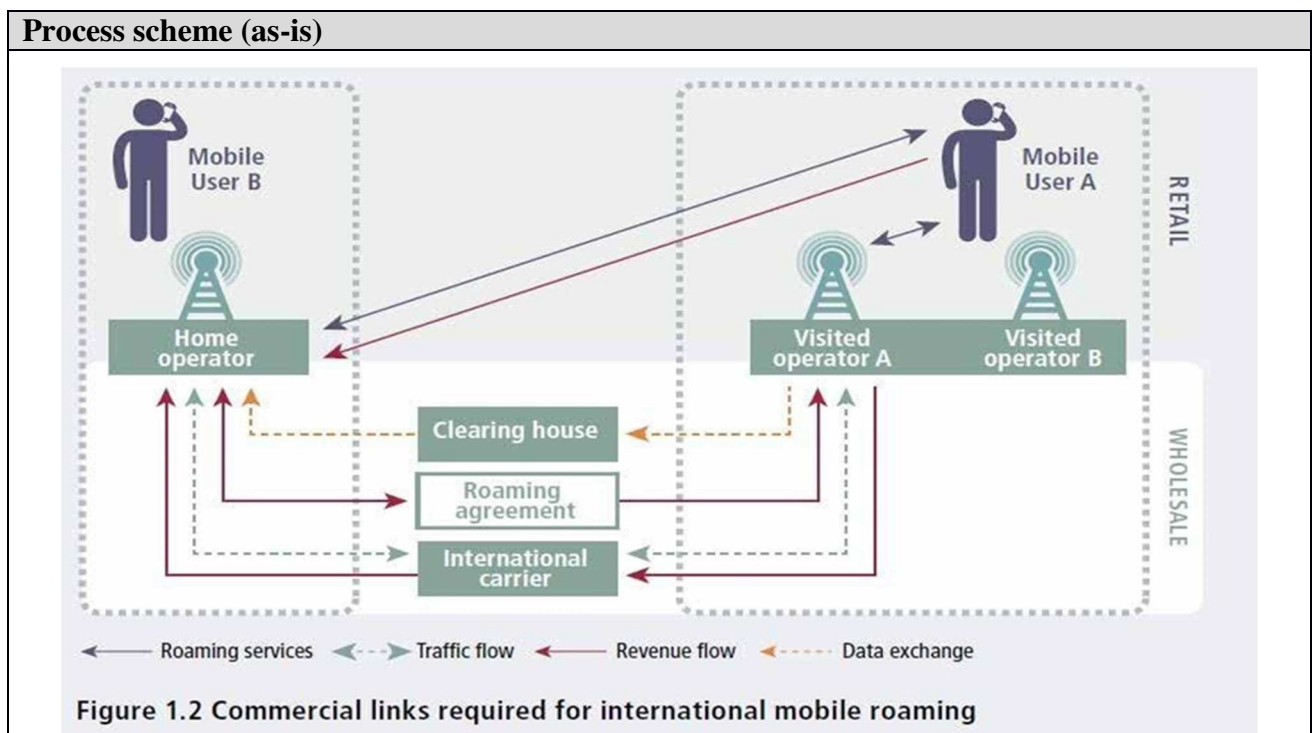
As for service providers it takes time and bears additional cost and efforts to reach customers.

Existing Flow (as-is)

Step	User Actions	System Actions
1.	MNO/MVNO determines a contact and negotiates with another international MNO/MVNO	n/a

錯誤! 所指定的樣式的文字不存在文件中。

Existing Flow (as-is)		
Step	User Actions	System Actions
2.	MNO/MVNO of one country signs roaming agreement with another international MNO/MVNO	n/a
3.	Mobile operators of both countries arrange interconnection of their networks and conduct necessary technical tests to provide roaming services	n/a
4.	Mobile operators of both countries exchange rates for their services and establish tariff plans for own subscribers	Tariff plans are published on operator's server
5.	Mobile subscribers choose/buy tariff plans via operator's user interface (web account or application) and travel abroad	Mobile subscribers of Home operator are registered in the network of Visited operator on arrival
6.	Mobile operators render roaming services based on agreed terms	n/a
7.	Mobile operators exchange invoices and make settlements	n/a



Data and information (as-is)		
Data	Type	Description
1		
2		

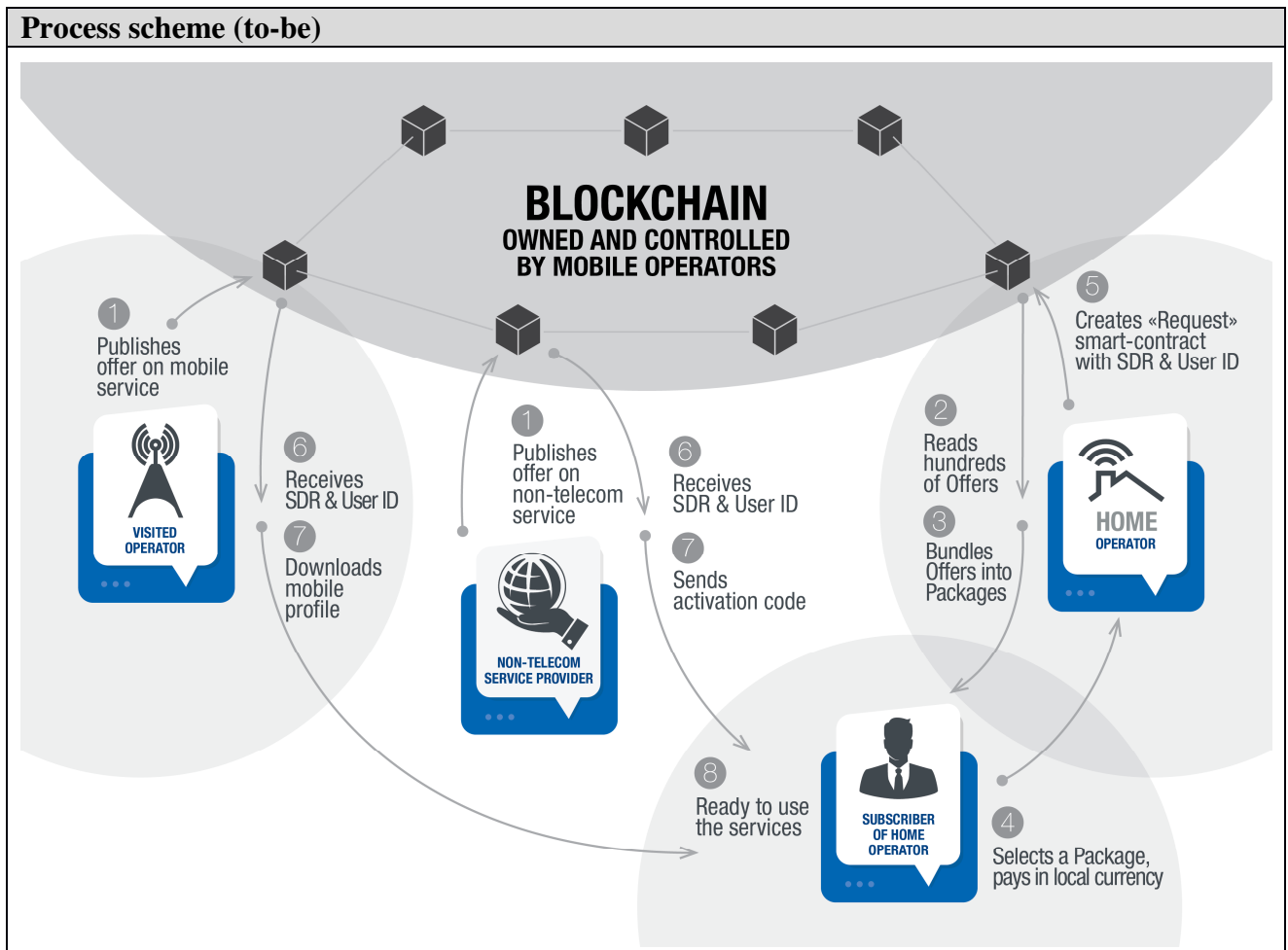
錯誤! 所指定的樣式的文字不存在文件中。

Participants and their roles (as-is)		
Actor	Type/Role	Description
1	MNO/MVNO	Any mobile network operator or mobile virtual network operator providing its own subscribers with international roaming services
2	Mobile subscribers	Mobile subscribers consuming international roaming services

Section 3 Expected process

Expected Flow (to-be)		
Step	User Actions	System Actions
1.	Any MNO/MVNO (Visited operator) and/or service provider (SP) publishes Offer on its own mobile services/non-telecom services onto Blockchain	“Offer” smart contract is created in Blockchain and system verifies it by all nodes
2.	Any MNO/MVNO joined Blockchain reads Offers published by another MNO/MVNO and/or SP via Blockchain account	n/a
3.	Any MNO/MVNO (Home operator) chooses Offers, edits them, bundles into packages and proposes them to its own subscribers with the use of User interface (web or app)	n/a
4.	Mobile subscriber of Home operator selects a package and pays for it in local currency	n/a
5.	Home operator creates Request smart contract with the user ID, other technical information and SDRt payment and sends it to Blockchain	“Request” smart contract is created in Blockchain and systems verifies it by all nodes
6.	Visited operator or SP receives request via Blockchain and accepts request supplying encrypted mobile profile data or SP’s code and other technical information necessary to get a service	“Accept” smart contract is created in Blockchain, system verifies it and matches to “Request” smart contract created at previous step
7.	Home operator downloads mobile profile received from Visited operator to subscriber’s multi-SIM via OTA platform and/or activates SP’s code.	n/a
8.	Mobile subscriber of Home operator is activated in the Visited operator’s network on arrival or in the SP’s system	n/a

Expected Flow (to-be)		
Step	User Actions	System Actions
9.	Visited operator or SP serves the subscribers of Home operator according to the contract purchased and reports service consumption to the Blockchain.	<p>Transactions about service consumption are published in Blockchain.</p> <p>SDR tokens are transferred from account of Home Operator to account of Visited Operator according to consumptions.</p>



Participants and their roles		
Actor	Type/Role	Description
1	MNO/MVNO	Any mobile network operator or mobile virtual network operator providing its own subscribers with international roaming services
2	Mobile subscribers	Mobile subscribers, consuming international roaming services
3	Nodes / Validators	Nodes ensure data integrity and provide consensus.

錯誤! 所指定的樣式的文字不存在文件中。

Participants and their roles		
Actor	Type/Role	Description
4	Service provider	<u>Any service provider, such as content providers, software vendors, insurance companies, logistic or transport organizations, hotels, etc.</u>

Data and information		
Data	Type	Description
1	Offer	Service with detailed description and price (in SDRt) published by any MNO/MVNO
2	Request	Order on an Offer selected by a subscriber of any MNO/MVNO
3	SDRt	SDR token – a stable token tied to SDR (Special Drawing Rights). This token is used for payment for services of mobile operators and service providers
4	User ID	Logical entity used to identify a user on a software, system, website or within any generic IT environment. It is used within any IT enabled system to identify and distinguish between the users who access or use it.
5	Mobile profile	Set of keys for secure registration of a SIM-module in the mobile network of Mobile Operator who owns this Mobile profile
6	Smart Contract	Computer protocol intended to digitally facilitate, verify, or enforce the negotiation or performance of a contract . Smart contracts allow the performance of credible transactions without third parties. These transactions are trackable and irreversible.
7	SP's code	Special digital code of service provider needed for service activation

Security and privacy
Sensitive information is encrypted. All transactions are signed by digital signatures of all participants. Personal data of end user dose not store in Blockchain. Only internal ID of end user is transmitted for further direct identification by Visited operator or SP in it's network/system.

Main Success Scenario
<ol style="list-style-type: none"> 1. Mobile operators and service providers interact directly and securely without agreements, intermediators and additional integration via smart contracts. 2. Any small and medium-sized MNO/MVNO and/or service provider becomes global in a very short period of time. 3. Mobile subscribers get high quality services from mobile operators and service providers at affordable rates.

Conditions (pre- or post-)
n/a

Performance needs
Fast transactions and confirmations from DLT system are necessary. Currently it takes 3-5 seconds of delay for transaction' confirmation and in average about 10 000 transactions per second, which is enough for all expected technical loads.

Legal considerations
n/a

Risks

Special Requirements
<ul style="list-style-type: none">- It is necessary for Home Mobile operator to produce and distribute Multi-Account SIM-cards or eSIMs among its subscribers;- It is necessary for Home Mobile operator to have OTA (over-the-air) platform to upload mobile profiles.

External References and Miscellaneous
https://wiki.blockchaintele.com/index.php/Main_Page https://wiki.blockchaintele.com/index.php/Use_cases#Global_coverage_with_local_rates_for_subscribers

Other Notes
Open questions: <ul style="list-style-type: none">• Settlement in SDRt is a subject of further study and implementation.

Automatic Discovery, Quote, Ordering and Settlement in a Mesh of Interconnected ICT Service Providers

Section 1: Summary

Use Case Summary			
Use Case ID:	ICT-002	Use Case Type:	<i>Vertical</i>
Submission Date:	July 14, 2019	Is Use Case supporting SDGs	<i>no</i>
Use Case Title:	Automatic Discovery, Quote, Ordering and Settlement in a Mesh of Interconnected ICT Service Providers	Domain:	1-c 3-f
Status of Case	PoC	Sub-Domain	<i>If necessary</i>
Contact information of person submitting/ managing the use-case	Shahar Steiff AVP New Technology E-mail address: ssteiff@pccwglobal.com Telephone number: +85263888875 Social media: Web site: www.pccwglobal.com		
Proposing Organization	PCCW Global Limited. Hong Kong		
Short Description	PoC conducted at MEF18 event that demonstrated Automatic Discovery, Quote, Ordering and Settlement in a Mesh of Interconnected ICT Service Providers resulting in a significant decrease in time compared to legacy manual processes.		
Long description	<p>On October 2018 a team of 7 Carriers (PCCW Global, Infonias, Liquid Telecom, Singtel, Sparkle, and Tata Communications) together with two technology partners (Cataworx and Clear Blockchain Technologies) has presented a PoC where the process of obtaining a quote, ordering of a service, invoicing for such service, invoice reconciliation and final settlement for service delivered through a partial mesh of interconnected carrier networks were conducted through an automated system.</p> <p>Each carrier network was operating a catalogue of available services and upon receiving an inquiry from its customer through an eNNI it would search the catalogue for a matching entry and return a price if found. If no matching entry was found, the catalogue would then initiate an inquiry to its neighbour eNNI connected carriers that will then repeat this process until a matching entry is found in one of the catalogues (or until a pre-defined threshold has been reached, either time, or number of hops). If a price is returned by an downstream catalogue, the originating catalogue would then mark the price up according to defined commercial rules, and provide a quote to the upstream catalogue. This cascade of inquiries and quotes eventually provides the ultimate customer a quote for an end-to-end service that may span across multiple carrier networks.</p> <p>Once the ultimate customer places an order – a cascade of orders is placed downstream with all participating carriers.</p>		

	<p>Once service is terminated – invoices are being generated by each carrier based on their measured utilization (a combination of time, throughput and SLA metrics) and is then being reconciled with the measurement of the neighbour eNNI carriers.</p> <p>Once reconciliation is complete – the invoices are settled.</p> <p>The above proceeds, when handled manually on Carriers’ legacy OSS/BSS platforms, may take weeks to complete.</p> <p>The PoC has demonstrated that the inquiry, quote and ordering take less than 30 seconds, and invoicing and reconciliation takes less than two minutes.</p> <p>This may result in a significant reduction in both time and HR, as not only that the process is accelerated, it is also automated.</p> <p>The information is exchanged through private permissioned ledgers between each pair of carriers and this is a flat-hierarchy architecture with no top-level orchestrator. Reflecting the commercial environment of the wholesale ICT market. There is complete isolation of information and visibility and no one has end-to-end visibility and control.</p>		
SDG in Focus (when applicable)	Goal 9: Build resilient infrastructure, promote sustainable industrialization and foster innovation		
Value Transfer:	The solution includes financial settlement between each pair of entities.	Number of Users:	Millions
Types of Users:	<p>End users: Private, Enterprise and Wholesale ICT SPs.</p> <p>ICT SPs: Connectivity SPs (carriers), Compute and Storage SPs (Public and Private Cloud).</p>		
Stakeholders	<p>End users: Ability to buy on-demand services. Ability to pay per-use.</p> <p>ICT SPs: Ability to deliver on-demand services and Yield new revenue from existing infrastructure.</p> <p>IoT SPs: Ability to use managed-services on-demand.</p>		
Data:	<p>Inquiry details, Quote details, Order details, Utilization records, SLA performance, Invoice details, Settled amount.</p> <p>The respective data models are service-type specific (connectivity DM differs from Compute DM that differs from Storage DM). The information is shared between the two eNNI partners only.</p> <p>Catalogue interaction will be through an API.</p> <p>End user interaction is expected to be through an intent-based interface.</p>		
Identification:	<p>This is a permissioned ledger. Only pre-accepted members can participate. Governance is managed through a board consisting of representatives of members of the ledger.</p>		
Predicted Outcomes:	<p>As demonstrated in the PoC – Manual processes replaced by automation significantly accelerate enabling a host of new applications that are currently dependent on best-effort, unmanaged, resources.</p>		

Overview of the Business Problem or Opportunity

Problem:

Most ICT services traverse more than one network domain. Each such network domain (a carrier network, a data centre, a radio link, an enterprise LAN) is typically operated by a different administration and is using different methods to transport, process and manage the flows of information.

It is very seldom that all administrations along the information flow path use a common language/process to define and manage their portion of the end to end path. Furthermore – it is very seldom that true end-to-end visibility and management is available across all administrations.

The typical process-flow is such that each two consecutive administrations along the end-to-end path have bilateral commercial and operational relations with each other that have overcome some of the differences in language/process. These relations are heavily dependent on manual processing of requests, manual provisioning of services, manual management, semi-manual invoicing and manual settlement. Such manual laden process-flow is time consuming and does not allow services to be activated on-demand but rather requires orders to be placed in advance, then be subject to delivery lead-times of weeks or months. For services that span across multiple administrations – the problem is further amplified as the service-related information now flows through a cascade/chain of bilateral agreements. Timelines stretch even further and management of the end to end service characteristics becomes very difficult.

Today's applications require resources to become available within minutes/seconds. Waiting months before establishing a video connection is not an option. While compute and storage resources are already available for on-demand consumption, and can be made ready for use within minutes or even seconds of notice, managed connectivity between the user and the compute/storage resources cannot be delivered instantly due to the reasons stated above. As a result – if managed connectivity was not made available in advance, the applications resort to the use of the public internet, which on one hand offers always-on any-to-any connectivity, but on the other hand offers no effective measures to manage the connectivity and guarantee performance.

Opportunity:

If we were able to guarantee quality of the end-to-end service, through management of each individual segment in the overall path, we could create an eco-system where all parties involved could benefit: The user will experience better quality services for which they will be willing (or forced) to pay. The ICT service providers will be able to charge for the use of their segments, provided that they manage and guarantee the quality and performance of their respective segment.

Why Distributed Ledger Technology?

ICT SPs operate in an equal-level playing field. There is no top-level administration that controls other administrations. Each ICT SP (administration) manages its own platforms as a “silo” using its own management system. No one will be willing to allow other administrations to administer their resources and services.

This creates a challenge when it comes to managing information flows across a chain of distributed administrations that have no hierarchy. That is where blockchain can play a role as a trusted mechanism to convey and manage information in a distributed environment. The fact that the information is owned by everyone and all nodes are at an equal hierarchical level makes it possible for administrations to exchange information related to services, and blockchain can then ensure integrity of the information across those multiple administrations.

The PoC has demonstrated how Quote, Order, Invoice, Reconciliation and Settlement information is exchanged across a chain of ICT SPs with timelines down to seconds on a per-pair of SPs basis, and minutes on a multi-SP environment.

Section 2: Current process

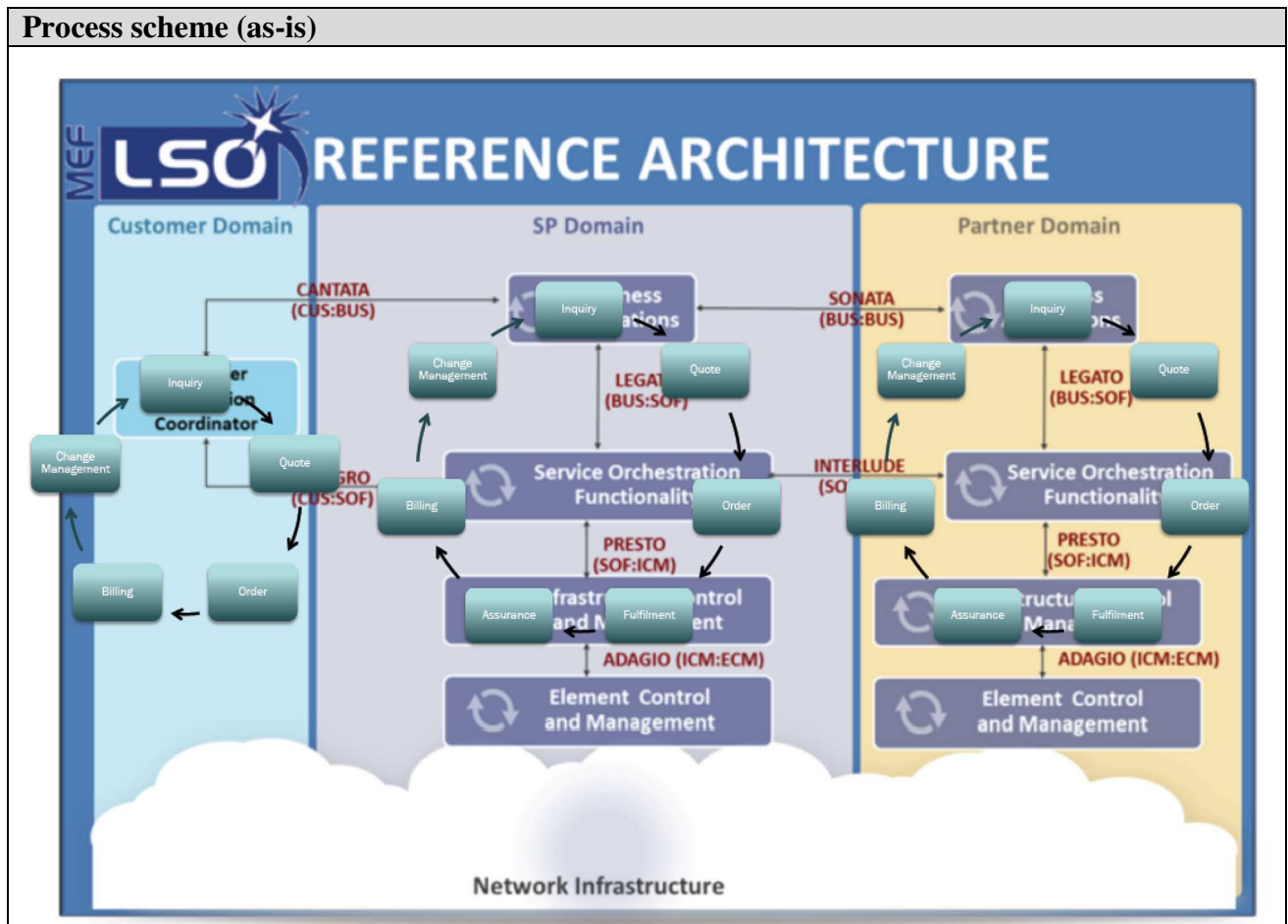
Current Solutions

Today there is no system offering end-to-end automation. There are automation platforms in existence that automate some (or all) of the lifecycle of services within a single administration, but each is confined to the limits of its own administration.

Existing Flow (as-is)

Step	User Actions	System (administration) Actions
1.	Make an Inquiry with an administration about availability and cost of a certain Service. User may send the same inquiry to multiple potential supplier administrations.	Manual processing of request. Analysis of the elements. Design a solution. Obtain cost of the solution-elements, including on-net (offered within the administration) and off-net (obtained from other administrations). Off-net inquiries trigger the same process with the downstream administration which may trigger additional processes with additional downstream administrations. The end result is that (if a solution is found and available) a Quote is returned to the User. This quote may include off-net quotes obtained from downstream administrations and may include mark-up of such quotes.
2.	Place an Order with the supplier administration.	Receive Order, send on-net elements of the order to provisioning, place order(s) for off-net elements with other administration(s). Those orders, once received by those other administration(s) may trigger additional orders with additional downstream administrations. Once the service has been provisioned and tested end to end it is handed-over to the user.
3.	Pay invoice on pre-agreed intervals (excluding SLA remedies)	Generate invoice on pre-agreed intervals based on agreement. Deduct SLA remedies if applicable. Pay invoices received from downstream administrations.

Existing Flow (as-is)		
Step	User Actions	System (administration) Actions
4.	Request termination of service from supplier administration (may be subject to term commitments).	Receive request for termination. Terminate on-net elements of service. Send termination requests to downstream suppliers for the off-net elements of service. The downstream supplier may then send termination requests to additional downstream suppliers. Off-net termination requests are subject to term commitments which do not necessarily correspond to the term commitment for the service ordered by the User.



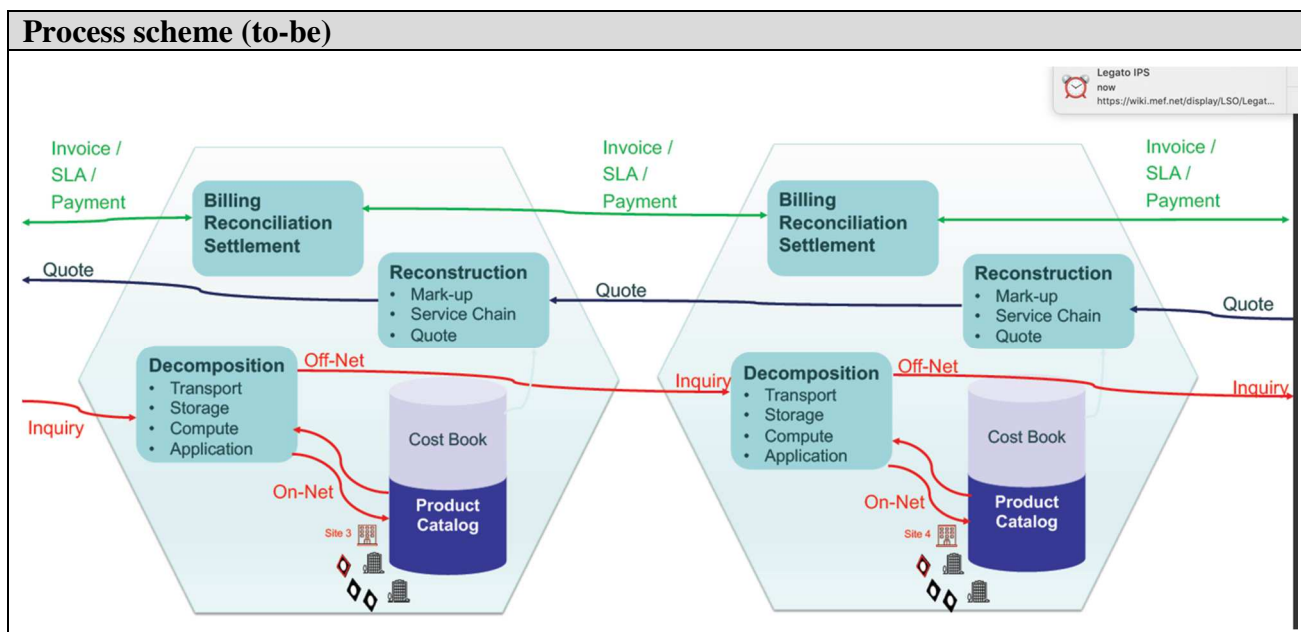
Data and information (as-is)		
Data	Type	Description
1	Documents	Cost books (Excel, PDF, on-line). Order forms (Excel, Fax, on-line). Invoices (PDF, on-line). Solution diagrams (Visio, PPT). Inventory management (on-line, Excel)
2	Payment transactions	Manual processing of invoices (that are generated automatically or semi-automatically)

Participants and their roles (as-is)		
Actor	Type/Role	Description
1	<i>Users</i>	An individual, and SME, a large enterprise, a Telecom carrier, Governments, Universities and any other entity that may buy ICT services from Administrations that supply ICT services.
2	<i>Administrations</i>	Entities that provide and sell ICT services.

Other Notes
<i>Any assumptions, issues</i>

Section 3: Expected process

Expected Flow (to-be)		
Step	User Actions	System Actions
1.a	Request a Quote for on-demand (Immediate or Delayed activation. No term commitment) using a portal	Automatic parsing of the requirement (possibly using an intent-based parser). Automatic quoting of on-net elements based on a product/service catalogue. Automatic request of a quote for off-net elements from downstream administrations. Return quote to user if end-to-end solution is found.
1.b	Activate an app based on a pre-existing rate schedule for on-demand services without term commitments.	Detect activation of app and initiate activation of services to support the app. Request activation of off-net elements from downstream administrations.
2.a	Request Activation of service based on Quote received.	Initiate activation of services to support the order. Request activation of off-net elements from downstream administrations.
2.b	(n/a)	
3.a	Request termination of service	Automatically terminate service and send termination requests to downstream administrations. Initiate invoicing for service based on commercial terms and measured usage (time, volume, bandwidth, distance etc.)
3.b	Close app	Automatically turn down the services that supported the app. send termination requests to downstream administrations. Initiate invoicing for service based on commercial terms and measured usage (time, volume, bandwidth, distance etc.)
4.	Pay invoice	Receive payment



Participants and their roles		
Actor	Type/Role	Description
1	Users	An individual, and SME, a large enterprise, a Telecom carrier, Governments, Universities and any other entity that may buy ICT services from Administrations that supply ICT services.
2	Administrations	Entities that provide and sell ICT services.

Data and information		
Data	Type	Description
1	Documents	On-net Catalogues, electronic quotes, electronic orders, SLA
2	Payment transactions	Blockchain based (may use crypto currency or FIAT currency)

Security and privacy
<ol style="list-style-type: none"> 1. Based on a Permissioned ledger. 2. Each pair of administrations runs a bilateral blockchain session. 3. Shared ledger used for failover, ZKP and reputation

Main Success Scenario + expected time line
PoC successfully presented at MEF18 event in October 2018.
On-going standardization work initiated at MEF.

Conditions (pre- or post-)
<ol style="list-style-type: none"> 1. Requires agreement of all involved parties on common Service definitions, Common Information and Data models and a common Process.

2. Plenty of Standardization work is still ahead of us.

Performance needs

The solution is based on off-the-shelf servers such as those offered by public cloud providers.

Legal considerations

This is automation of an existing process so there are no legal complexities that have not already been solved.

Governance of the code, ledger membership and IP rights requires agreement between participating administrations.

Risks

Not that I can think of.

Special Requirements

See “Conditions” above

External References and Miscellaneous

MEF 6.2, MEF 7.4, MEF MCM, MEF 50.1, MEF 55, ONF TAPI

Other Notes

Wholesale Voice Settlement

Section 1 Summary

Use Case summary			
Use Case ID:	ICT-003	Use Case Type:	Vertical
Use Case Title:	Wholesale Voice Settlement	Domain:	IT & Telco; Finance
Stakeholder:	Wholesale voice carriers		
Value Transfer:	Money transfer	N. of participants:	1000+
Data:	Carrier identities, commercial relationships, their terms, and settlement results are stored in DLT, some encrypted or hashed. CDRs (Call Detail Records/Call logs), settlement process are stored outside DLT but can be referenced by DLT		
Users:	Wholesale carriers		
Identification:	Carriers are identified, however the peers of a specific bilateral relationship are not necessarily specifically known, only their membership in the global carrier group is known. Some information about the voice call supply chain may be shared.		
Predicted Outcomes:	Implementation of global DLT system will automate existing manual processes and consolidate (currently disperse) systems, thus streamlining, increasing efficiency and reducing costs. It will also reduce human errors and time spent resolving disputes, further improving efficiency. Through transparency and short turnaround - fraud may be reduced and dissolved.		

Overview of the Business Problem or Opportunity
Though the underlying systems involved in bilateral wholesale voice trade are mostly automated, some of the handoff of information from one system to another is not yet fully automated, and the settlement and dispute resolution are handled mostly through a labour intensive manual process. Through DLT technology, certain elements of this process may be streamlined and automated.
Why Distributed Ledger Technology?
<p>The commercial interactions between carriers are carried out in an environment of mutual suspicion. Settlement between disparate systems operated by mutually-suspecting commercial entities requires either a trusted, neutral (but paid for), third party, or a lengthy laborious bilateral manual process to resolve commercial disputes and reach settlement.</p> <p>Certain bilateral processes, primarily in the mobile communications sector, use a centralized party to resolve disputes and reach settlement. However – the charges levied by such centralized parties amount to a significant (and growing) part of the ever thinning margins of the wholesale mobile business. The margins in the wholesale voice business are even thinner than those in the wholesale mobile business, rendering a paid-for centralized entity a non-viable solution.</p> <p>In addition to that – the current wholesale voice business process involves multiple disparate functions, each performed by a disparate system, that still require sequential treatment of data and feeding the output of one system to the next system in the sequence (e.g. CDR collection on voice</p>

switch fed to rating engine that feeds the invoicing systems that leads to manual dispute-resolution that eventually leads to settlement).

A DLT solution may be used for multiple purposes:

1. Create a common interchange and enforcement mechanism without a trusted third party.
2. Integration of the functionality of multiple disparate systems into a single system that performs a streamlined process that rates the CDRs, compares with the bilateral carrier, identifies and resolves disputes, then settles the account.
3. Settlement can be handled through automated FIAT currency transactions by APIs to Banks' swift clearing systems, through automated DLT transactions of electronic versions of FIAT currencies, or through crypto-currency transactions using either an existing crypto-currency or one that will be created for the purpose of wholesale telecommunications settlements.

Section 2 Current process

Current Solutions

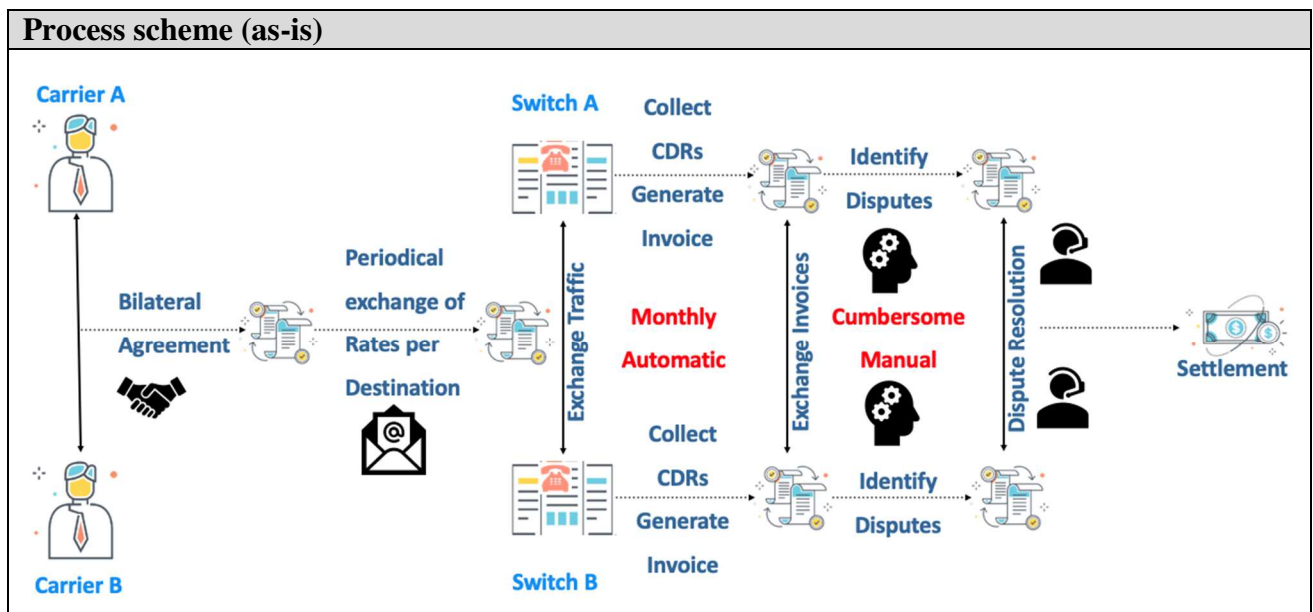
Carriers have rating systems which perform automated analysis of CDRs, and automatically generate invoices. Such invoices are only seldom accepted by the recipient carrier and are often disputed. Disputed invoices then undergo a manual dispute resolution process during which both carriers negotiate, try to identify the reasons for the disputes and then reach settlement. It is not uncommon to see such negotiations stretch over months and at times both parties end up in court.

It is estimated that the wholesale voice industry as a whole is spending an order of magnitude of the equivalent of 10 years of HR every month resolving disputes.

Existing Flow (as-is)

Step	User Actions	System Actions
1.	Telephone call is made	CDR is collected and stored (Automatic)
2.	(periodical, typically monthly)	<p>All collected CDRs are rated based on comparison of the destination of the call with the agreed upon rate to that destination, and multiplication of the rate by the duration of the call, taking into account agreed upon rounding of duration (typically on a 1 second or 5 second basis). (Automatic)</p> <p>CDRs are being separated to inbound (for which the carrier is expecting to be paid by the bilateral carrier) and outbound (which the carrier expects to be invoiced for by the bilateral carrier). (Automatic)</p>

Existing Flow (as-is)		
Step	User Actions	System Actions
3.	(periodical, typically monthly)	<p>All rated inbound CDRs are collected and summed up. An invoice is generated for the sum of all rated CDRs and sent to the bilateral carrier. (Automatic)</p> <p>All rated outbound CDRs are collected and summed up but no invoice is generated. The sum of those rated CDRs is the amount the carrier is expecting to be invoiced for by the bilateral carrier. (Automatic)</p>
4.	(periodical, typically monthly)	Invoices are exchanged between the bilateral carriers. (Automatic or semi-auto).
5.	An invoice from a bilateral carrier is received.	Compare the invoice received with the amount the carrier is expecting to be invoiced for (as calculated in step 3 above) and identify differences, if any exist. (Manual)
6.	If disputes are found	Negotiate with bilateral carrier. Try to identify the reason for the dispute. Agree which carrier made the error that caused the dispute. Re-calculate the invoice amount after correcting the error and repeat step 5 above. (Manual)
7.	Disputes have been resolved or no disputes	Settle the outstanding undisputed invoices. (Manual)



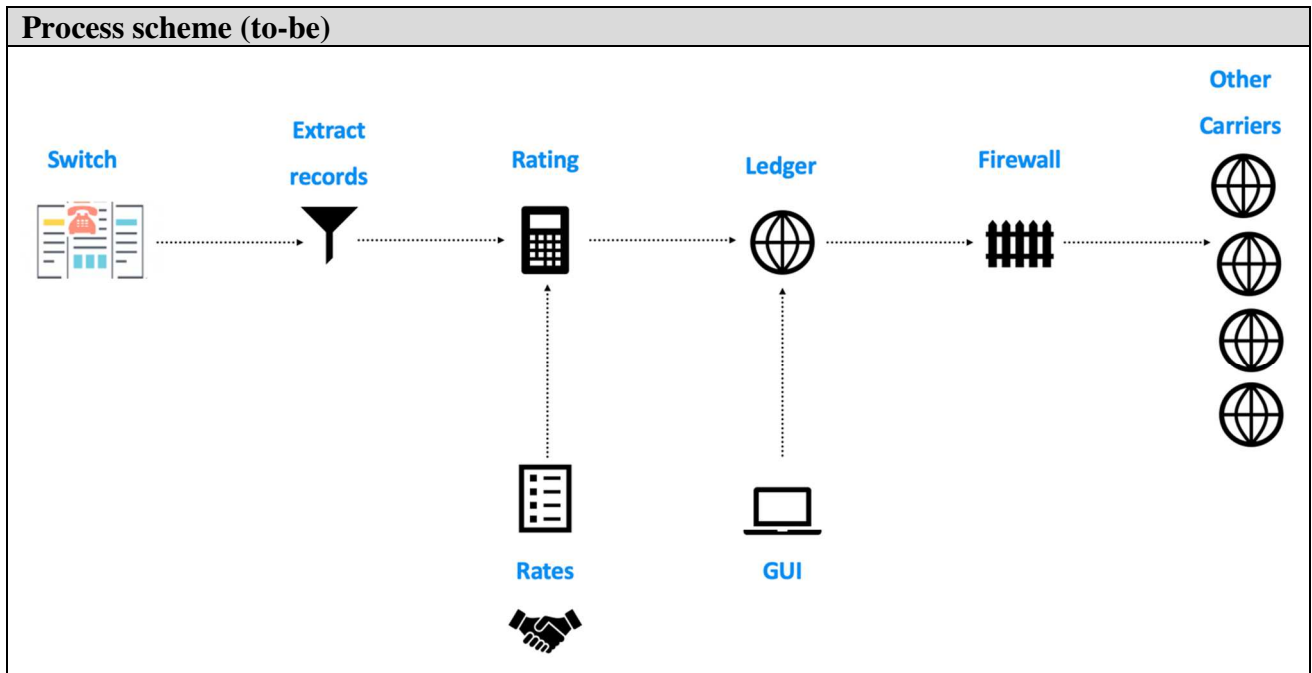
Data and information (as-is)		
Data	Type	Description
1	<i>Documents</i>	<p>MSA (Master Service Agreement) or T+C (Terms and Conditions). Defines the rules of engagement, credit and payment terms, dispute resolution methods, rating methods, governing law.</p> <p>CDR – Call Detail Record. Includes information of the originating telephone number, the destination telephone number, the identity of the carrier sending the call, the identity of the carrier receiving the call, call start time, call end time (or call duration), result of call (success, fail, RNA [Ring No Answer]).</p> <p>Rate-Sheet. Periodically exchanged between bilateral carriers and defining the rate-per-minute of voice traffic sent to certain destinations.</p> <p>Rated-CDR. Excludes information of source and destination telephone numbers. Includes the commercial value of the call through multiplication of the call duration by the agreed upon rate appearing in the current bilateral rate sheet.</p>
2	<i>Payment transactions</i>	<p>Invoice. The sum of all rated CDRs for a period.</p> <p>Settlement. Payment of undisputed Invoices.</p>

Participants and their roles (as-is)		
Actor	Type/Role	Description
1	<i>Originating Carrier</i>	The carrier sending voice traffic to another carrier.
2	<i>Recipient Carrier</i>	The carrier receiving voice traffic from another carrier.

Other Notes
<p>In a bilateral relationship a carrier can be both an Originating Carrier and a Recipient Carrier.</p> <p>A Carrier can have relationships with multiple carriers.</p> <p>Tripartite relations may exist where two carriers agree to exchange traffic through a third, transit, carrier. In such case there may be separate agreements between the three carriers (Originating, Transit, Recipient).</p>

Section 3 Expected process

Expected Flow (to-be)		
Step	User Actions	System Actions
1.	Telephone call is made	CDRs are collected and stored (Automatic)
2.	(periodical, PoC has proven that the period can be as short as 15 seconds)	<p>All collected CDRs are rated based on comparison of the destination of the call with the agreed upon rate to that destination, and multiplication of the rate by the duration of the call, taking into account agreed upon rounding of duration (typically on a 1 second or 5 second basis). (Automatic)</p> <p>CDRs are being separated to inbound (for which the carrier is expecting to be paid by the bilateral carrier) and outbound (which the carrier expects to be invoiced for by the bilateral carrier). (Automatic)</p>
3.	(periodical, same frequency as above)	<p>All rated inbound CDRs are collected and summed up. An invoice is generated for the sum of all rated CDRs and sent to the bilateral carrier using a bilateral DLT. (Automatic)</p> <p>All rated outbound CDRs are collected and summed up but no invoice is generated. The sum of those rated CDRs is the amount the carrier is expecting to be invoiced for by the bilateral carrier. (Automatic)</p>
4.	An invoice from a bilateral carrier is received through DLT.	Compare the invoice received with the amount the carrier is expecting to be invoiced for (as calculated in step 3 above) and identify differences, if any exist. (Automatic)
5.	If disputes are found	Apply a dispute-resolution algorithm (described separately). (Automatic with certain exceptions)
6.	Disputes have been resolved or no disputes	Settle the outstanding undisputed invoices using DLT. (Automatic or Manual)



Participants and their roles		
Actor	Type/Role	Description
1	<i>Originating Carrier</i>	The carrier sending voice traffic to another carrier.
2	<i>Recipient Carrier</i>	The carrier receiving voice traffic from another carrier.
3	<i>Bank</i>	In certain scenarios DLT settlement may initiate an API call to a Bank's SWIFT service to perform FIAT currency payment.
4	<i>IMF (International Monetary Fund)</i>	In certain scenarios DLT settlement may take place using an electronic version of SDR (a currency defined by IMF).

Data and information		
Data	Type	Description
1	<i>Documents</i>	<p>MSA (Master Service Agreement) or T+C (Terms and Conditions). Defines the rules of engagement, credit and payment terms, dispute resolution methods, rating methods, governing law.</p> <p>CDR – Call Detail Record. Includes information of the originating telephone number, the destination telephone number, the identity of the carrier sending the call, the identity of the carrier receiving the call, call start time, call end time (or call duration), result of call (success, fail, RNA [Ring No Answer]).</p> <p>Rate-Sheet. Periodically exchanged between bilateral carriers and defining the rate-per-minute of voice traffic sent to certain destinations.</p> <p>Rated-CDR. Excludes information of source and destination telephone numbers. Includes the commercial value of the call through multiplication of the call duration by the agreed upon rate appearing in the current bilateral rate sheet.</p>
2	<i>Payment transactions</i>	<p>Invoice. The sum of all rated CDRs for a period exchanged thru DLT.</p> <p>Settlement. Payment of undisputed Invoices performed through DLT.</p>

Security and privacy
<p>1. The use case assumes a <i>Permissioned Private DLT</i> that uses <i>PoA (Proof of Authority)</i> with multiple signatures and <i>DBFT consensus mechanism</i>.</p> <p>2. Access to the platform is only allowed to Carriers identified as such by other carriers and is administered by a <i>SPV (Special Purpose Vehicle)</i> that includes Carriers members of the DLT.</p>

Main Success Scenario
<p>Interoperable private blockchains</p> <ul style="list-style-type: none"> • <i>Between bilateral Carriers, using interoperable protocol.</i> • <i>Bilateral transactions are carried out on a bilateral DLT (one per pair).</i> <p>Open-source shared blockchain</p> <ul style="list-style-type: none"> • <i>Failover to Shared blockchain.</i> • <i>Permissioned network using open-source Ethereum nodes.</i> • <i>Also used for dispute resolution using ZKP for Transit traffic.</i> <p>Pluggable Commercial Logic and Ingestion</p> <ul style="list-style-type: none"> • <i>Single shared network with variety of products and interactions</i> • <i>Dispute resolution may use AI/Heuristics algorithms and can include failover to manual resolution based on criteria.</i>

- *Dispute resolution algorithms may differ on a partner-Carrier and destination basis.*

Conditions (pre- or post-)

1. *Participating Carrier must be accepted to the DLT platform based on criteria set forth by SPV.*
2. *Participating Carrier must provide a Dedicated or Virtual compute resource that meets the requirements set forth by SPV, either on-premise or in Cloud, and load the software provided by SPV on the compute resource.*

Performance needs

Based on estimated volume of traffic and number of bilateral connections the compute resources can be sized with accuracy. The PoC has proven that an off-the-shelf standard configuration VM in public clouds is sufficient for the task.

Legal considerations

1. *The PoC is implemented using existing legal contracts between Carriers.*
2. *The use of crypto-currency is an option that may be subject to certain legal restrictions in specific geographies,*

Risks

International Wholesale Voice trading (IDD) is a well-established business that has its roots in the days of national operators (PTTs), and although it has gone through deregulation in most countries, it is one of the most supervised and controlled environments in the telecom business. Automation of elements of this business, through use of DLT or without it, does not change the legal frameworks the IDD business is established upon.

The only exception to the above is the use of DLT to settle commercial transactions using Crypto-Currencies. Reason being that such transactions may be banned in some geographies due to local regulations. Said risk can be mitigated as Crypto-Currency is not a mandatory method for settlement, and as discussed above, settlement can also be executed through API based automated SWIFT bank transactions, through electronic versions of FIAT currencies or even manually as is done today.

Other risks may be related to acceptance of suspicious carriers to the DLT, who may try to perform fraudulent IDD transactions. This is an existing risk and the move to DLT-based automation will neither increase the risk itself, nor will it risk an increase in its occurrence. On the contrary – DLT-based automation will shorten the cycles by which fraudulent activity can be identified, thus reducing the exposure in case of such activities. Add to that the reputation management that is embedded into DLT which will allow carriers to easily verify the reputation of a potential bilateral partner prior to establishing a business relation.

Special Requirements

The PoC has demonstrated that no special requirements exist. Considering a full-scale system – the compute resources and data transport resources required for proper functionality of the system are within what is currently available off-the-shelf as public-cloud based VMs or commercially and publicly available blades and servers to be installed in a private cloud or a data centre. Connectivity wise – the PoC has demonstrated that a 1Gbps link should suffice to carry the entire global CDR exchange between carriers using DLT.

External References and Miscellaneous

Other Notes

Appendix 1

Domains for use cases categorization

Vertical:

1. Finance
 - a. Financial management & accounting
 - b. International & interbank payments
 - c. Clearing and settlement
 - d. Reduction of Fraud
 - e. Financial messaging
 - f. Asset lifecycles and history
 - g. Trade finance
 - h. Regulatory compliance & audit
 - i. AML/KYC
 - j. Insurance
 - k. Peer-to-peer transactions
2. Healthcare
 - a. Pharma
 - b. Biotechnology
 - c. Medicine
3. Industries
 - a. Manufacturing
 - b. Energy
 - c. Chemical
 - d. Retail
 - e. Real estate
 - f. IT and telco
 - g. Supply chain management
 - h. Transportation and logistic
4. Government and public sector
 - a. Taxes
 - b. Government and non-profit transparency
 - c. Legislation, compliance & regulatory oversight
 - d. Voting
 - e. Taxation and customs
 - f. Intellectual property management

Horizontal:

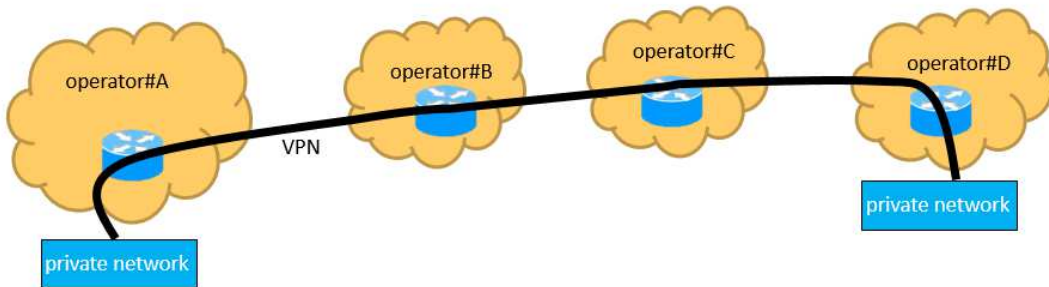
1. Identity Management
 2. Security Management
 - a. Public Key Infrastructure
 3. Internet of Things
 4. Data storage (Inter-organizational data management)
-

Distributed Ledger based Online Trading System for Cross-domain VPN Provision

Section 1 Summary

Use Case Summary			
Use Case ID:	ICT-004	Use Case Type:	Vertical
Use Case Title:	Distributed Ledger based Online Trading System for Cross-domain VPN Provision	Is Use Case supporting SDGs	Yes
		Domain:	Industries
Status of Case	Proof-of-Concept	Sub-Domain	IT and telco
Contact information of person submitting/ managing the use-case	<p><i>Xinpeng Wei</i> wexinpeng@huawei.com</p> <p><i>Bingyang Liu</i> liubingyang@huawei.com</p>		
Proposing Organization	<i>Huawei</i>		
Short Description	This use case is a proposal for utilizing DLT-based online trading system for cross-domain VPN (Virtual Private Network) provision services, which enables a custom to purchase cross-domain VPN service on-demand and flexibly.		
Long description	<p>A virtual private network (VPN) extends a private network across a public network, and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. Usually the VPN connection will cross one or more networks operated by different operators, and the operators should have SLAs between each other to setup of end-to-end VPN connection for customers, the process of setup VPN could take a very long time both due to technology issues and SLA issues between operators, but because the VPNs are usually static provisioned and once setup it will maintained for a very long time, so the time taken for VPN setup is acceptable.</p> <p>But as the new cases that VPN should be setup in a more flexible and on-demand way, the existing solution for VPN setup is no longer acceptable, because it is usually unknown which operator's network to traverse and whether the en-route operators has SLAs between each other.</p> <p>This document provides a use case that DLT is used for on-demand VPN connection setup across different domains.</p>		
SDG in Focus (when applicable)	<p>Goal 9: Industry, Innovation and Infrastructure</p> <p>9.3 Develop quality, reliable, sustainable and resilient infrastructure, including regional and transborder infrastructure, to support economic development and human well-being, with a focus on affordable and equitable access for all.</p>		

Value Transfer:	Token which is used to pay for VPN service.	Number of Users:	thousands
Types of Users:	enterprise, residential customer network, network operator		
Stakeholders	enterprise, residential customer network, network operator		
Data:	1. The data that VPN user sends to network operator for VPN provision. 2. The Service Level Agreement signed between different network operators.		
Identification:	Full identification of each entity is required.		
Predicted Outcomes:	1. Minimize time to negotiate VPN provision process. 2. Eliminate the need of pre-sign SLAs between customer and service providers.		

Overview of the Business Problem or Opportunity
<p>Currently in order to establish VPN connection across more than one operators' network, because the QoS of VPN connection needs to be provided along the whole connection path, so operators should have SLAs between each other and each operator makes its own provisions for the VPN connection. The process of setup VPN could take a very long time both due to technology issues and SLA issues between operators, but because the VPNs are usually static provisioned and once setup it will maintained for a very long time, so the time taken for VPN setup is acceptable.</p>  <p>Figure 1: VPN connection across different operators' network</p> <p>But for the new use case of on-demand VPN connection, the existing solution is hard to satisfy the requirements for the following reasons:</p> <ol style="list-style-type: none"> 1. The on-demand VPN is very dynamic, and it is hard to predict with network it will traverse. 2. The on-demand VPN could only exist for a short time, e.g. only a few days, so the time cost of establishing such as connection should be low enough.
Why Distributed Ledger Technology?
<p>DLT is to build a trust infrastructure, which helps the private network to set up trust relationship with the network providers for establishing VPN connection, and enables fast on-line trading between them to realize automatic VPN provision.</p>

Section 2 Current process

Current Solutions

The current solution depends on the operators' SLA pre-signed with each other.

Existing Flow (as-is)

Step	User Actions	System Actions
1.	The VPN user (owner of private network) sends out a request to the operator it directly connected to establish VPN connection between private networks.	N/A
2.	The network operator provision its own network devices to provide VPN connection and ask for the next network operator to provide VPN connection in its network according to SLA, and so on until the end-to-end VPN is fully provisioned.	N/A

Process scheme (as-is)

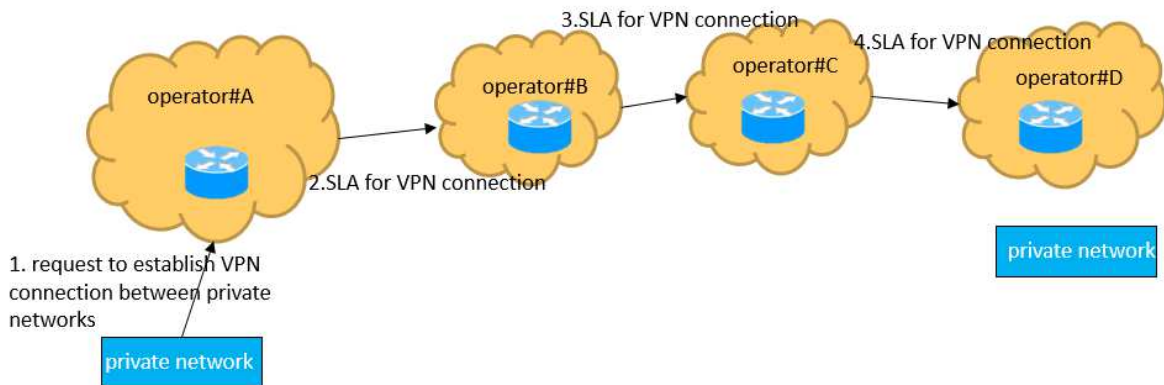


Figure 2: VPN provision procedure

Data and information (as-is)

Data	Type	Description
1	VPN provision request	The data that VPN user sends to network operator for VPN provision.
2	SLA	The Service Level Agreement signed between different network operators.

Participants and their roles (as-is)		
Actor	Type/Role	Description
1	VPN user	The entity who wants to establish VPN connection.
2	Network operator	The entity who operates the network.

Other Notes
N/A

Section 3 Expected process

Expected Flow (to-be)		
Step	User Actions	System Actions
1.	VPN user gets en-route networks' information between private networks.	Ledger records networks' information about the VPN service they can provide.
2.	VPN user sends request to network operator's smart contract to establish VPN connection between private networks. The VPN configuration-related parameters will be included in the request.	Ledger checks the VPN user is authorized to send out the transaction, and the target network operator's smart contract exist. If true, DLT record the transaction.
3	Network operator gets VPN configuration-related parameters from the ledger.	Ledger provides VPN configuration-related parameters information to network operator.
4	Network operator acknowledges VPN service.	Ledger records network operator's transaction for VPN service acknowledge.

Process scheme (to-be)

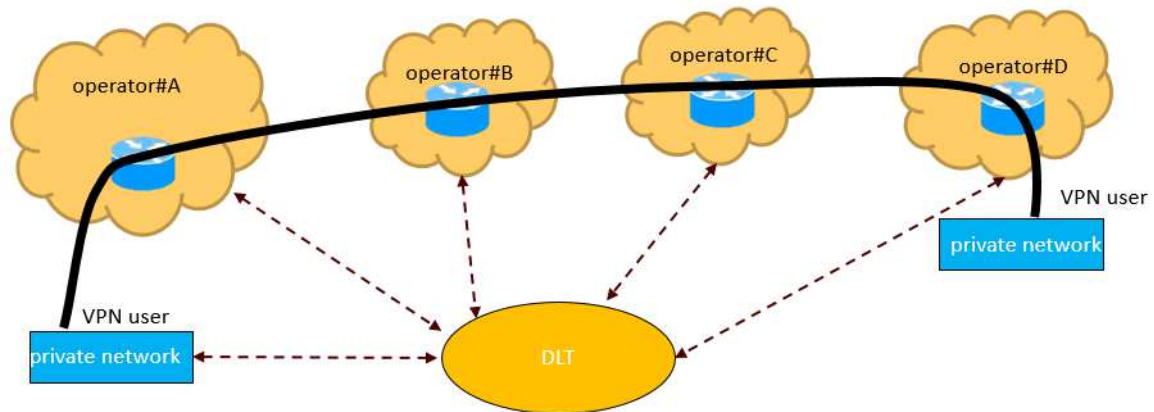


Figure 3: Overview of DLT and VPN Provision System

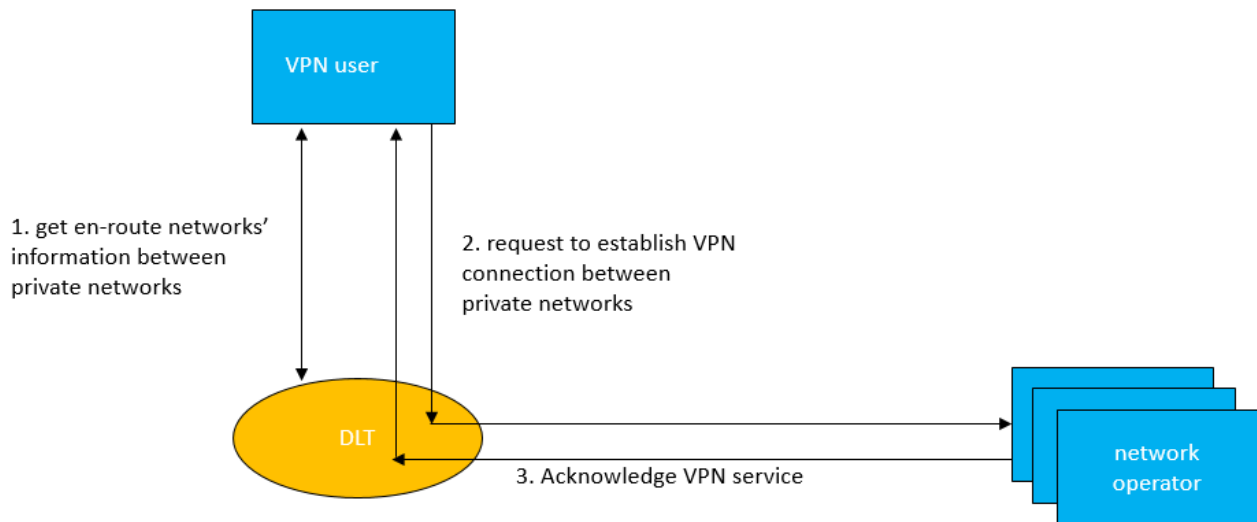


Figure 4: Procedures of VPN Provision Service

Participants and their roles

Actor	Type/Role	Description
1	VPN user	The entity who wants to establish VPN connection.
2	Network operator	The entity who operates the network.

Data and information

Data	Type	Description
1	Token account	Token representing money value. It is used to transfer value between VPN users and network operator.

Data and information		
Data	Type	Description
2	Service request transactions	The VPN users use service request transaction to ask for VPN provision service from network operators, and payment for the service will also be included.
3	VPN service information	The information is maintained at the smart contract in ledger, it includes the SLA that the network operator can provide for VPN provision.
4	Network-related information	Each network provides its own network information to the Ledger, this information is used by VPN users to figure out the en-route networks that the VPN connection will traverse.
5	VPN configuration-related parameters	These parameters are used to configure VPN connection properly, the VPN user decide these parameters and the Ledger will record these parameters.
6	VPN service acknowledge transaction	This transaction is used by network operator to accept the VPN provision request from VPN user.

Security and privacy
1. The network operator's service information recorded in DLT system should be trustable.

Main Success Scenario
1. All information exchange and payments occur in Distributed Ledger in automatic mode. 2. Payment and service are exchanged without human intervention.

Conditions (pre- or post-)
1. The token must be created in some way. 2. All parties are connected to DLT system. 3. All parties should have a recognizable identity.

Performance needs
1. Transactions processing near real time; 2. 24/7/365 availability; 3. Volume of transactions > 1000 TPS.

Legal considerations
N/A

Risks
1. DLT-related security risk.

Special Requirements
N/A

External References and Miscellaneous
N/A

Other Notes
N/A

Appendix 1

Domains and subdomains for use cases categorization

Vertical:

1. Finance
 - a. Financial management & accounting
 - b. International & interbank payments
 - c. Clearing and settlement
 - d. Reduction of Fraud
 - e. Financial messaging
 - f. Asset lifecycles and history
 - g. Trade finance
 - h. Regulatory compliance & audit
 - i. AML/KYC
 - j. Insurance
 - k. Peer-to-peer transactions
2. Healthcare
 - a. Pharma
 - b. Biotechnology
 - c. Medicine
3. Industries
 - a. Manufacturing
 - b. Energy
 - c. Chemical
 - d. Retail
 - e. Real estate
 - f. IT and telco
 - g. Supply chain management
 - h. Transportation
 - i. Agriculture
4. Government and public sector
 - a. Taxes
 - b. Government and non-profit transparency
 - c. Legislation, compliance & regulatory oversight
 - d. Voting
 - e. Taxation and customs
 - f. Intellectual property management
 - g. Land Registries

Horizontal:

1. Identity Management
2. Security Management
 - a. Public Key Infrastructure

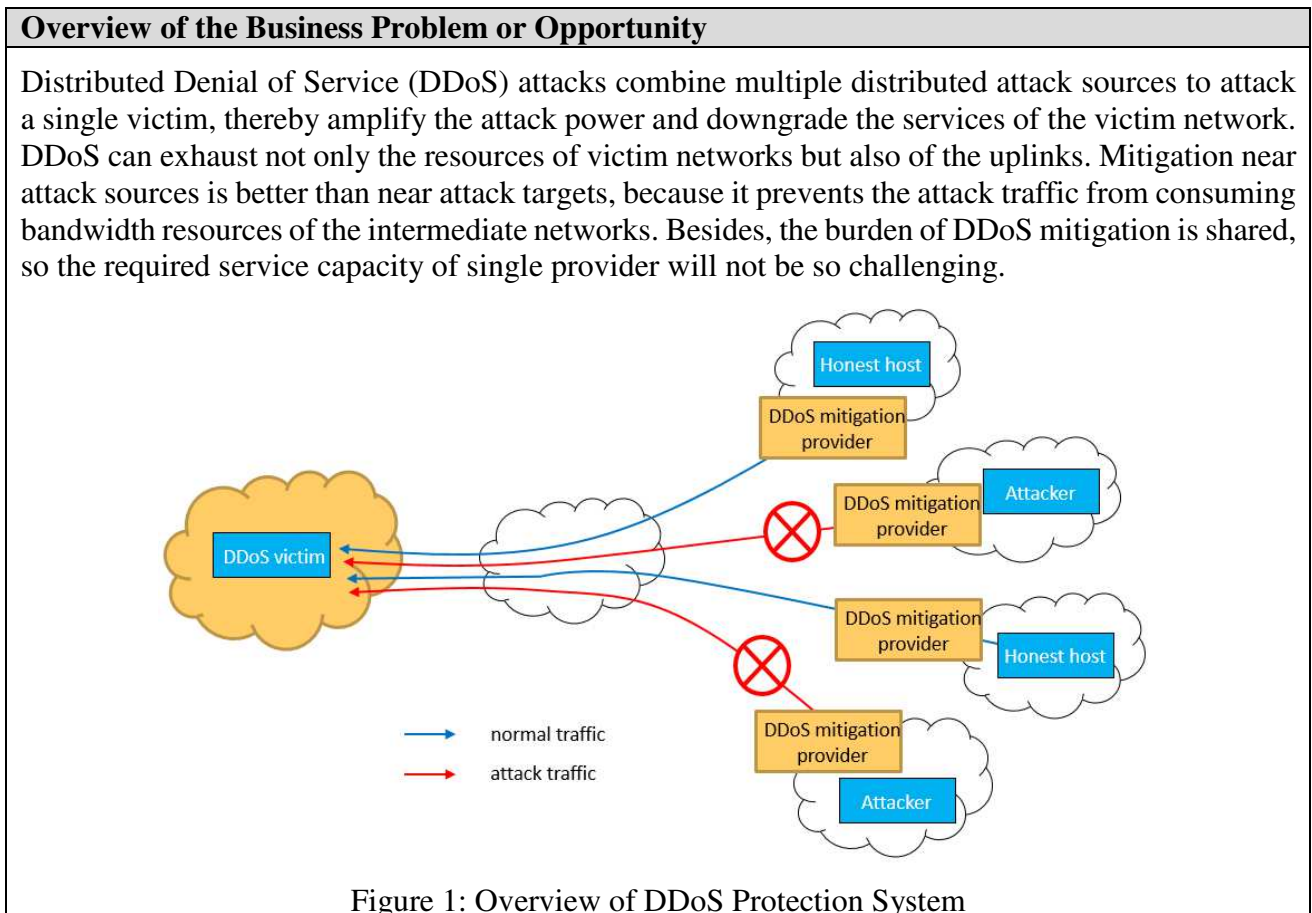
3. Internet of Things
4. Data processing, storage and management
 - a. Data Validation (includes provenance)

Distributed Ledger based Online Trading System for DDoS Mitigation Services

Section 1 Summary

Use Case Summary			
Use Case ID:	ICT-005	Use Case Type:	Vertical
Use Case Title:	Distributed Ledger based Online Trading System for DDoS Mitigation Services	Is Use Case supporting SDGs	Yes
		Domain:	Industries
Status of Case	Proof-of-Concept	Sub-Domain	IT and telco
Contact information of person submitting/ managing the use-case	<i>Xinpeng Wei</i> wexinpeng@huawei.com <i>Bingyang Liu</i> liubingyang@huawei.com		
Proposing Organization	<i>Huawei</i>		
Short Description	This use case is a proposal for utilizing DLT-based online trading system for DDoS mitigation services, which enables a victim network to on-demand purchase DDoS mitigation services close to the attack sources.		
Long description	This use case describes how DLT is used in DDoS mitigation service. Distributed Denial of Service (DDoS) attacks combine multiple distributed attack sources to attack a single victim, thereby amplify the attack power and downgrade the services of the victim network. DDoS mitigation service aims at mitigating DDoS attacks for the victim network. By using DLT, it's much easier to mitigate attack at the point of attack sources, and prevents the attack traffic from consuming bandwidth resources of the intermediate networks.		
SDG in Focus (when applicable)	Goal 9: Industry, Innovation and Infrastructure 9.3 Develop quality, reliable, sustainable and resilient infrastructure, including regional and transborder infrastructure, to support economic development and human well-being, with a focus on affordable and equitable access for all.		
Value Transfer:	Tokens which is used to pay for DDoS Mitigation service	Number of Users:	thousands
Types of Users:	Network operators, OTT (Over The Top), Internet users, enterprise, residential customer network		

Stakeholders	Network operators, OTT, Internet users, enterprise, residential customer network
Data:	<p>Token balance to each account.</p> <p>Service smart contract: Each DDoS mitigation service provider has a service smart contract to accept service requests from DDoS victim. Service smart contract include information about the service and price that DDoS mitigation service provider can provide.</p> <p>IP prefix-related information: The DLT records information about IP prefix and AS (Autonomous System) numbers, so given an IP prefix the corresponding AS number can be retrieved. By using these information, the DDoS victim can find the DDoS mitigation service provider when the IP address of attack source is identified.</p>
Identification:	Full identification of each entity is required.
Predicted Outcomes:	<ol style="list-style-type: none">1. Minimize time to negotiate DDoS mitigation service.2. Eliminate the need of pre-sign SLAs between customer and service providers.



However, near-source DDoS mitigation requires a business model that the victim network to purchase mitigation services from multiple providers close to the multiple source networks, which can be any of the tens of thousands of autonomous systems (ASes). There are two challenges:

First, the victim network has to set up business relationship with the remote providers, who may be unknown to the victim;

Second, different attacks have different sources, and thus require setting up business relationship with different providers. Due to the challenges, existing mitigation services are typically provided closed to the victim networks.

Why Distributed Ledger Technology?

DLT is to build a trust infrastructure, which helps the victim network to set up trust relationship with the remote providers, and enables fast on-line trading between them to start DDoS mitigation as soon as possible.

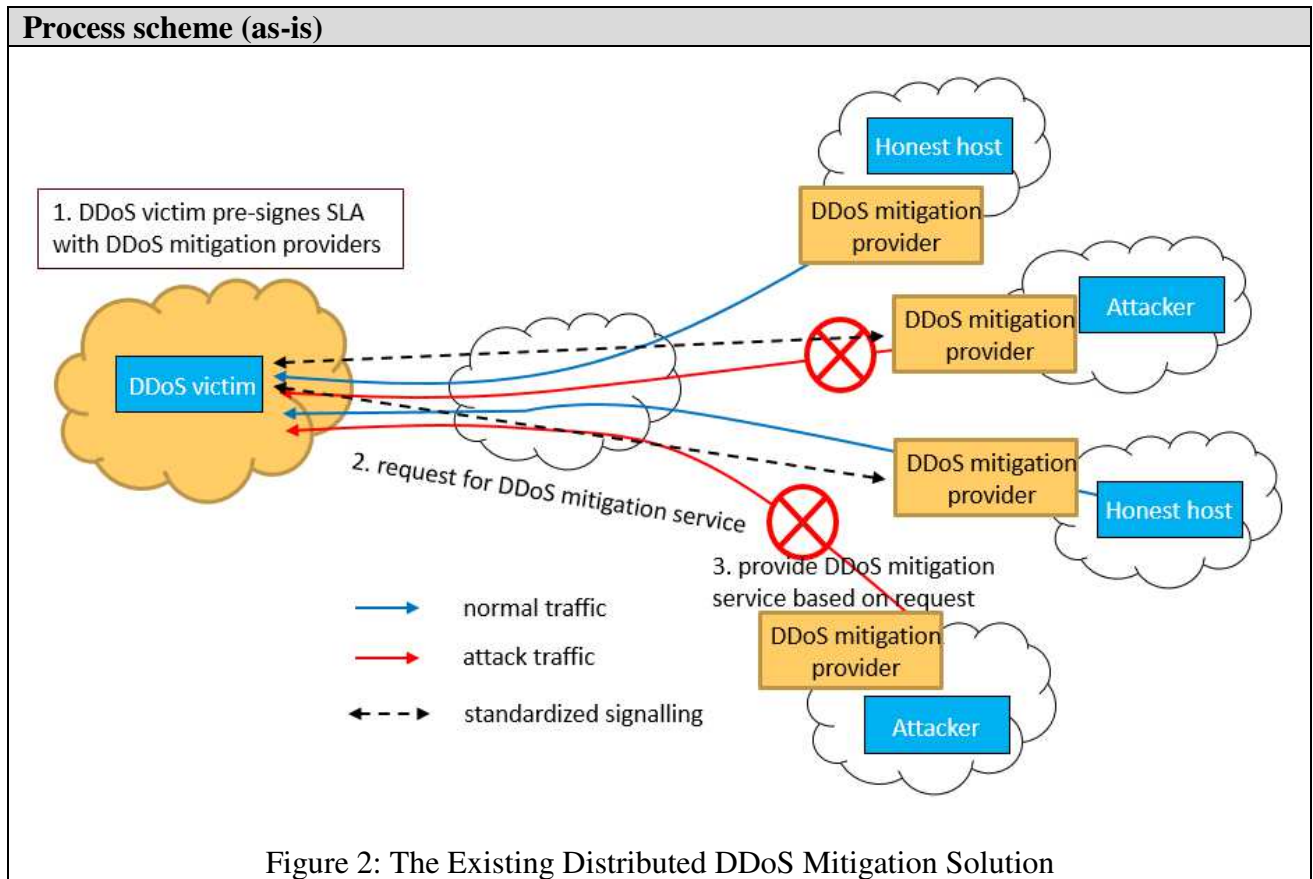
Section 2 Current process

Current Solutions

In the current solution, victim network has to set up business relationship with the DDoS mitigation service providers, and when the DDoS attack happens, the victim network sends request to the specific DDoS mitigation service provider.

Existing Flow (as-is)

Step	User Actions	System Actions
1.	DDoS victim pre-signs SLA with DDoS mitigation providers	N/A
2.	Request for DDoS mitigation service	N/A
3	Provide DDoS mitigation service based on request	N/A



Data and information (as-is)		
Data	Type	Description
1	DDoS mitigation service request	The victim send this request to service provider for DDoS mitigation service.

Participants and their roles (as-is)		
Actor	Type/Role	Description
1	DDoS victim	The entity who suffers from DDoS attack. Any entities connected to Internet could be a DDoS victim. E.g. ISP, enterprise, residential customer network, OTT etc.
2	DDoS mitigation provider	The entity who provide DDoS mitigation service. Usually, it is a network provider.

Other Notes
N/A

Section 3 Expected process

Expected Flow (to-be)		
Step	User Actions	System Actions
1.	DDoS victim initiates a transaction to DDoS mitigation provider's smart contract to request for DDoS mitigation service.	DLT checks the DDoS victim is authorized to send out the transaction, and the target DDoS mitigation provider's smart contract exist. If true, DLT record the transaction.
2.	DDoS mitigation provider evaluates DDoS victim's credibility verifying that the DDoS victim has the ownership of the attacked IP address.	N/A
3	DDoS mitigation provider initiates a transaction with the DDoS victim to agree to provide DDoS mitigation server.	DLT checks the transaction sent by DDoS mitigation provider is valid, and then record the transaction. After that the DDoS mitigation provider's smart contract will be executed, and token will be transferred from DDoS victim's account to DDoS mitigation provider's account.

Process scheme (to-be)

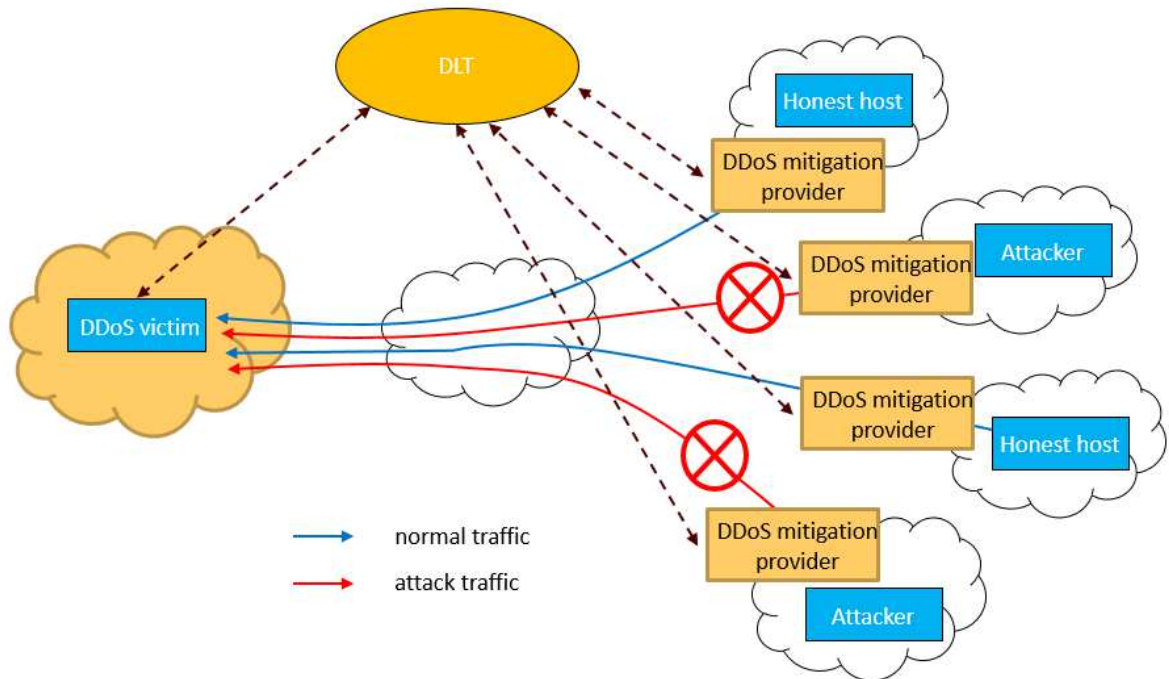


Figure 3: Overview of DLT and DDoS Mitigation System

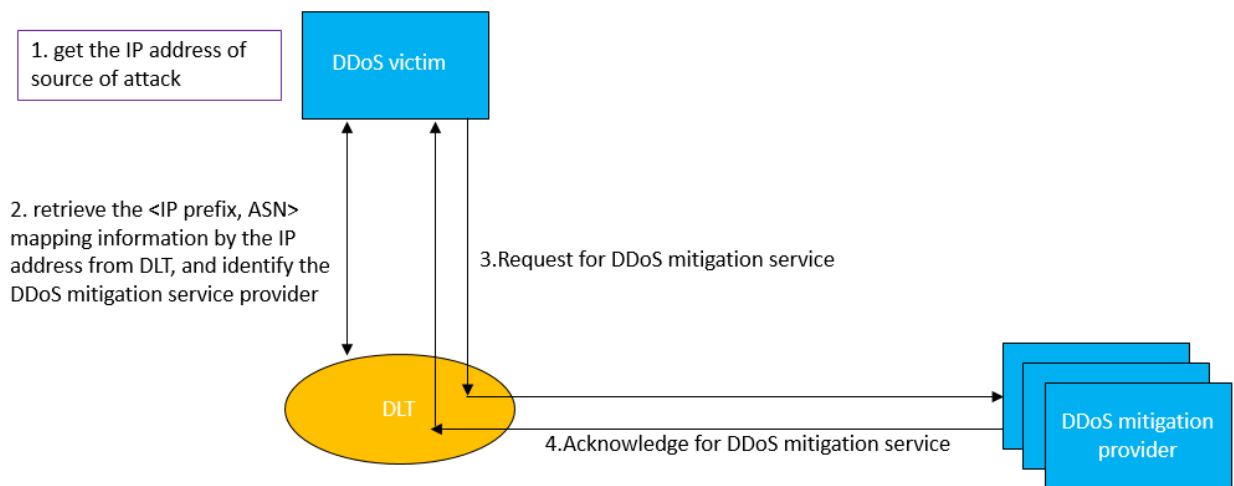


Figure 4: Procedures of DDoS Mitigation Service

Participants and their roles		
Actor	Type/Role	Description
1	DDoS victim	The entity who suffers from DDoS attack. Any entities connected to Internet could be a DDoS victim. E.g. ISP, enterprise, residential customer network, OTT etc.

Participants and their roles		
Actor	Type/Role	Description
2	DDoS mitigation provider	The entity who provide DDoS mitigation service. Usually, it is a network provider.

Data and information		
Data	Type	Description
1	token	Token representing money value. It is used to transfer value between DDoS victims and DDoS mitigation providers.
2	Service request transactions	The DDoS victim use service request transaction to ask for DDoS mitigation service from DDoS mitigation service provider, and payment for the service will also be included.
3	Service acknowledge transactions	The DDoS mitigation service provider use service acknowledge transaction to agree for DDoS mitigation service to DDoS victim.
4	Service smart contract	Each DDoS mitigation service provider has a service smart contract to accept service requests from DDoS victim. Service smart contract include information about the service and price that DDoS mitigation service provider can provide.
5	IP prefix-related information	The DLT records information about IP prefix and AS numbers, so given an IP prefix the corresponding AS number can be retrieved. By using these information, the DDoS victim can find the DDoS mitigation service provider when the IP address of attack source is identified.

Security and privacy
1. The DDoS mitigation provider's service ability recorded in DLT system DDoS mitigation provider should be trustable.
2. The IP prefix-related information recorded in DLT system should be trustable.

Main Success Scenario
1. All information exchange and payments occur in Distributed Ledger in automatic mode.
2. Payment and service are exchanged without human intervention.

Conditions (pre- or post-)
1. The token must be created in some way.
2. All parties are connected to DLT system.
3. All parties should have a recognizable identity.

Performance needs
1. Transactions processing near real time; 2. 24/7/365 availability; 3. Volume of transactions > 1000 TPS.
Legal considerations
N/A
Risks
1. DLT-related security risk.
Special Requirements
N/A
External References and Miscellaneous
N/A
Other Notes
N/A

Appendix 1

Domains and subdomains for use cases categorization

Vertical:

1. Finance
 - a. Financial management & accounting
 - b. International & interbank payments
 - c. Clearing and settlement
 - d. Reduction of Fraud
 - e. Financial messaging
 - f. Asset lifecycles and history
 - g. Trade finance
 - h. Regulatory compliance & audit
 - i. AML/KYC
 - j. Insurance
 - k. Peer-to-peer transactions
2. Healthcare
 - a. Pharma
 - b. Biotechnology
 - c. Medicine
3. Industries
 - a. Manufacturing
 - b. Energy
 - c. Chemical
 - d. Retail
 - e. Real estate
 - f. IT and telco
 - g. Supply chain management
 - h. Transportation
 - i. Agriculture
4. Government and public sector
 - a. Taxes
 - b. Government and non-profit transparency
 - c. Legislation, compliance & regulatory oversight
 - d. Voting
 - e. Taxation and customs
 - f. Intellectual property management
 - g. Land Registries

Horizontal:

1. Identity Management
2. Security Management
 - a. Public Key Infrastructure

3. Internet of Things
4. Data processing, storage and management
 - a. Data Validation (includes provenance)

VisionNG DLT for Number Assignment, Services and Number Portability

Section 1: Summary

Use Case summary			
Use Case ID:	ICT-006	Use Case Type:	Vertical
Use Case Title:	VisionNG DLT for number assignment, services and number portability	Domain:	Telecommunications
Stakeholder:			
Value Transfer:	Yes, currently not in use	N. of participants:	3
Data:	Contractual rules, chain of contracts, services type		
Users:	30000		
Identification:	You can participate anonymously only for specific services		
Predicted Outcomes:	Fast assignment, number and service portability with legacy fall back on DNSSec		

Overview of the Business Problem or Opportunity
Fast and scalable system for service and number portability
Why Distributed Ledger Technology?
There is no current solution for global number and service portability that provides fast cost effective and scalable technology that provides for global services deployment.

Section 2: Current process

Current Solutions
There are some parts available that provide some services like number resolution, but don't support any contractual system like number assignment or portability

Existing Flow (as-is)		
Step	User Actions	System Actions
1.	Manual interaction	Manual action via operator
2.		

Process scheme (as-is)
Single regions Sparse service

錯誤! 所指定的樣式的文字不存在文件中。

Data and information (as-is)		
Data	Type	Description
1	Documents	Manual, physical paper work
2	Payment transactions	Billing for services

Participants and their roles (as-is)		
Actor	Type/Role	Description
1	Telecommunications operators	Provide numbering resources and services
2	Users	Request and receive resources and services from operators

Other Notes

Section 3: Expected process

Expected Flow (to-be)		
Step	User Actions	System Actions
1.	Interact with the system via contract backed by smart contracts	Issues keys, and store and executes smart contract roles, stores record and syncs with legacy systems
2.		

Process scheme (to-be)

Participants and their roles		
Actor	Type/Role	Description
1	Telecommunications operators	Make arrangements to enable keys to be issued, to store and execute smart contract roles, to store records and sync with legacy systems
2	Users	Interact with the system via contract backed by smart contracts

Data and information		
Data	Type	Description
1	Transactions	Assignments, reclamations, changes, etc.

錯誤! 所指定的樣式的文字不存在文件中。

Data and information		
Data	Type	Description

Security and privacy		
Entities are represented by cryptographic keys and specific smart contract are issued per region / service		

Main Success Scenario		
Number resource is available on Global Cloud DLT DApp platforms for global application and service delivery		

Conditions (pre- or post-)		
----------------------------	--	--

Performance needs		
Current number portability solutions take days where semi distributed system like DNS take milliseconds		

Legal considerations		
Must comply with national regulatory requirements		

Risks		
-------	--	--

Special Requirements		
Implementing Number and services management platform to interact with the existent DLT systems		

External References and Miscellaneous		
---------------------------------------	--	--

Other Notes		

Appendix 1

Domains for use cases categorization

Blockchain/DLT offers capabilities suitable for a wide variety of uses and purposes in many different domains and types of applications. There are 2 main types of DLT-based applications and services:

- Vertical applications and services (e.g., telco, fintech, supply chain, energy)
- Horizontal (infrastructural) applications and services (e.g., data usage control, identity management, security)

Vertical use cases could be categorized to domains according to the list below (note, that the list is not exhaustive):

1. Finance
 - a) Financial management & accounting
 - b) International & interbank payments
 - c) Clearing and settlement
 - d) Reduction of Fraud
 - e) Financial messaging
 - f) Asset lifecycles and history
 - g) Trade finance
 - h) Regulatory compliance & audit
 - i) AML/KYC
 - j) Insurance
 - k) Peer-to-peer transactions
2. Healthcare
3. Voting
4. Smart manufacturing
5. Intellectual property management (Digital rights management)
6. Supply chain and inventory management
7. Media
8. Energy
9. Government and public sector
 - a) Taxes
 - b) Government and non-profit transparency
 - c) Legislation, compliance & regulatory oversight
10. Real estate
11. Taxation and customs

Horizontal use cases could be categorized to domains according to the list below:

1. Identity Management
2. Cybersecurity
3. Big data

錯誤! 所指定的樣式的文字不存在文件中。

4. Data storage (Inter-organizational data management)
5. IoT
