Blockchain Technology for Industry Number Management & Portability

NICC Open Forum
7th November 2018

Phil Bone — Number Management Enterprise Architect
Girish Mahajan — Number Management Solutions Architect

© British Telecommunications plc 2017

Topics

Problem statement
Blockchain: “Fit” with numbering
Proof of Concept

© British Telecommunications plc 2017

Problem Statement

© British Telecommunications plc 2017

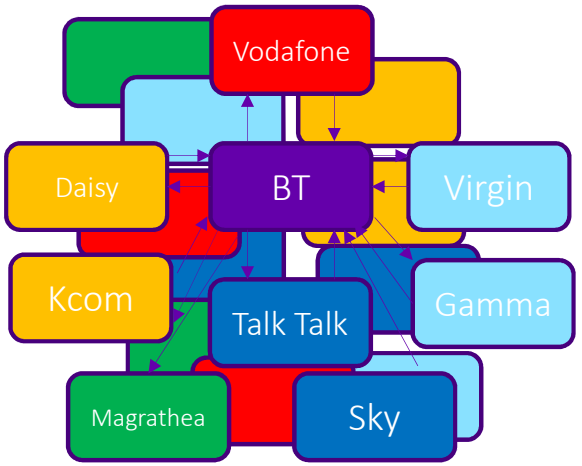
Industry Number Portability: Problem Statement

The current process is "unfit for purpose"

Industry ***Number Port Executive Steering Group*** (NPESG), led by the ***Office of the Telecoms Adjudicator*** (OTA2), has a remit to strategically improve geographic number port processes and has accepted that current processes are "unfit for purpose" for the following reasons.

The current bi-lateral (CP to CP) process:

- Is complex and ambiguous.
- Delivers a poor customer experience with extended lead times.
- Cannot cope with high demand.
- Is unsuited to large numbers of CPs porting numbers (c400 CPs currently).
- Is unable to support a complex porting stakeholder community.
- Does not adequately support complex porting scenarios (e.g. multi-number).
- Is unsuitable for future Fixed – Mobile convergence needs.
- Does not support "Direct Routing" call delivery to ported numbers.



© British Telecommunications plc 2017

Number Management & CLI Authentication: Requirements

Two additional use cases

In addition to number portability, Ofcom have presented two additional use cases:

- Telephony number resource management: the management of telephone number resources on allocation to Comms Providers (CPs) and Mobile Network Operators (MNOs). Current capabilities and processes are sub-optimal and lack automation. Issues include records inaccuracies and the need for a significant human resource management overhead on the part of both Ofcom and CPs to administer process.
- CLI authentication: the ability to identify and record individual telephone numbers or number ranges deemed to be associated with known fraudulent activity in accordance with *Secure Telephone Identity Revisited* (STIR) objectives. This presents a new challenge.

Although production functional requirements for these two use cases are currently unclear, a basic reference to each has been incorporated into the blockchain "Proof of Concept" architecture (discussed later).

© British Telecommunications plc 2017

Blockchain: “Fit” with numbering

© British Telecommunications plc 2017

Overview of Blockchain as a Technology Base for Number Portability

A "Foundational" technology

*"Blockchain is **not a "disruptive" technology**, which can attack a traditional business model with a lower-cost solution and overtake incumbent firms quickly. Blockchain is instead **a foundational technology**: it has the potential to create **new foundations for our economic and social systems**."*

Marco Iansiti & Karim R. Lakhani, Harvard Business Review 2017

Blockchain provides an alternative to traditional methods of managing industry number management and number port process; it does not eliminate the *need* for the process.

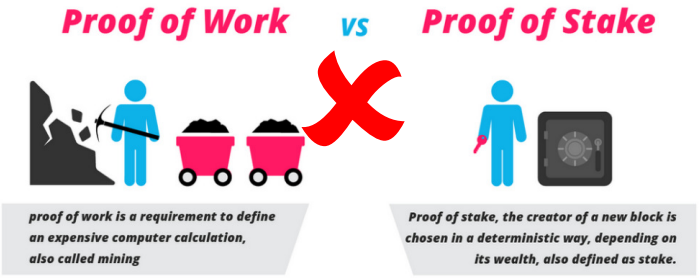
© British Telecommunications plc 2017

This is not about “Bitcoin”!

We propose to use blockchain foundational fabrics that have been developed to support industry use cases involving peer to peer transactions that are NOT financially orientated.

The key differences over public cryptocurrency blockchain architectures are:

- No bitcoin transactions, bitcoin mining operations nor any direct financial incentives for completing transactions.
- As a consequence, there is no “proof of work” or “proof of stake” requiring complex and expensive computer processing power to crack an algorithmic “puzzle”, to create a block and “win the prize”.
- Closed, “permissioned” participant consortium.



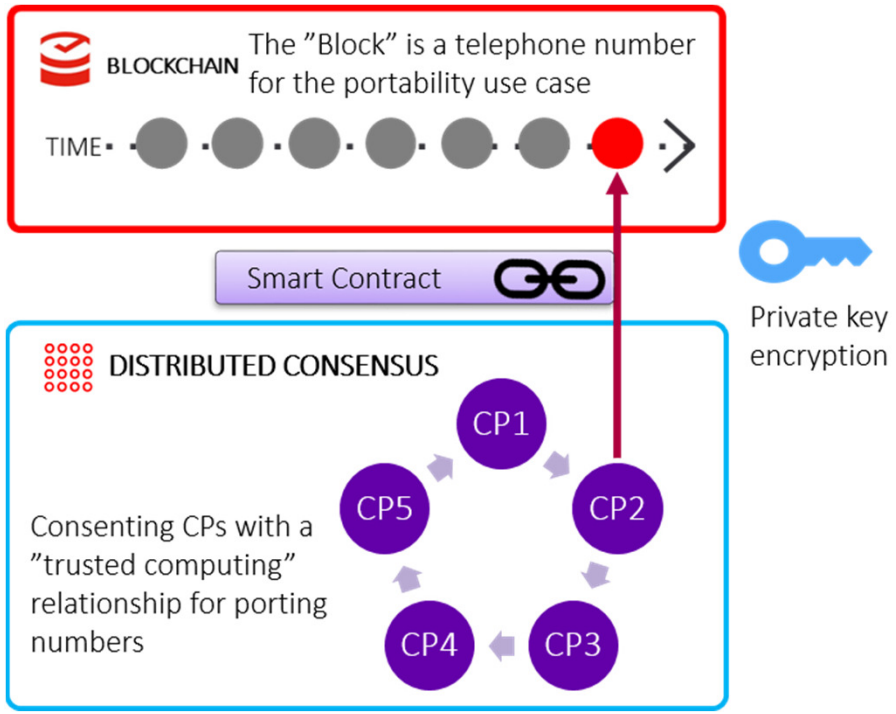
© British Telecommunications plc 2017

Overview of Blockchain as a Technology Base for Number Portability

Exploiting the key blockchain technology concepts

A blockchain-based number port process architecture will exploit five of the key concepts that characterise the technology:

1. **Distributed consensus**
2. **The Blockchain ledger**
3. **Smart contracts**
4. **Trusted computing**
5. **Signature transaction verification**



Participating CPs in the "closed (trusted computing) consortium" consent to transactional updates made to the digital asset block (the telephone number) via an agreed "Smart Contract" invoked via "Private Key" access & encryption. Updated blocks contain a "signature" to verify a transaction is valid.

© British Telecommunications plc 2017

Proof Of Concept

© British Telecommunications plc 2017

Blockchain for Number Portability: "Proof of Concept" (POC)

As a radically different approach, we need to prove it will work

As a radical technology, the PoC aims to showcase that blockchain, as a technology, is supportive of the numbering use cases identified. Some of the criteria it will demonstrate includes:

- Centralised (Ofcom) governance over the CP community.
- Use of digital asset (block) ledgered data to drive smart contract logic e.g. use of ledgered digital asset data to determine number port use case scenarios and initiate porting transactions with the relevant CP.
- Ability to manipulate ledgered records in a relational database-like manner for e.g. MIS purposes.
- Maintenance of participant profile characteristics to drive, for example, peer to peer smart contract number port transaction logic.
- Ability to link multiple transaction steps to form a process : e.g. the ability to link together the series of transactions between a gaining and losing CP to complete the port of a number.
- "Block locking" i.e. ledgered asset locking during a porting order transaction between two consenting participants.

© British Telecommunications plc 2017

It's a "Proof of Concept" not a "Prototype"!

Expectations for the PoC

- The *Proof of Concept* is not a prototype solution (requirements for which will have to be agreed in detail with the various stakeholder communities).

- It is intended to trial characteristics of blockchain technology to assess its potential and suitability for numbering.

- It provides representative use case functionality to demonstrate the potential of the technology.

© British Telecommunications plc 2017

PoC Technology

Linux Hyperledger Fabric

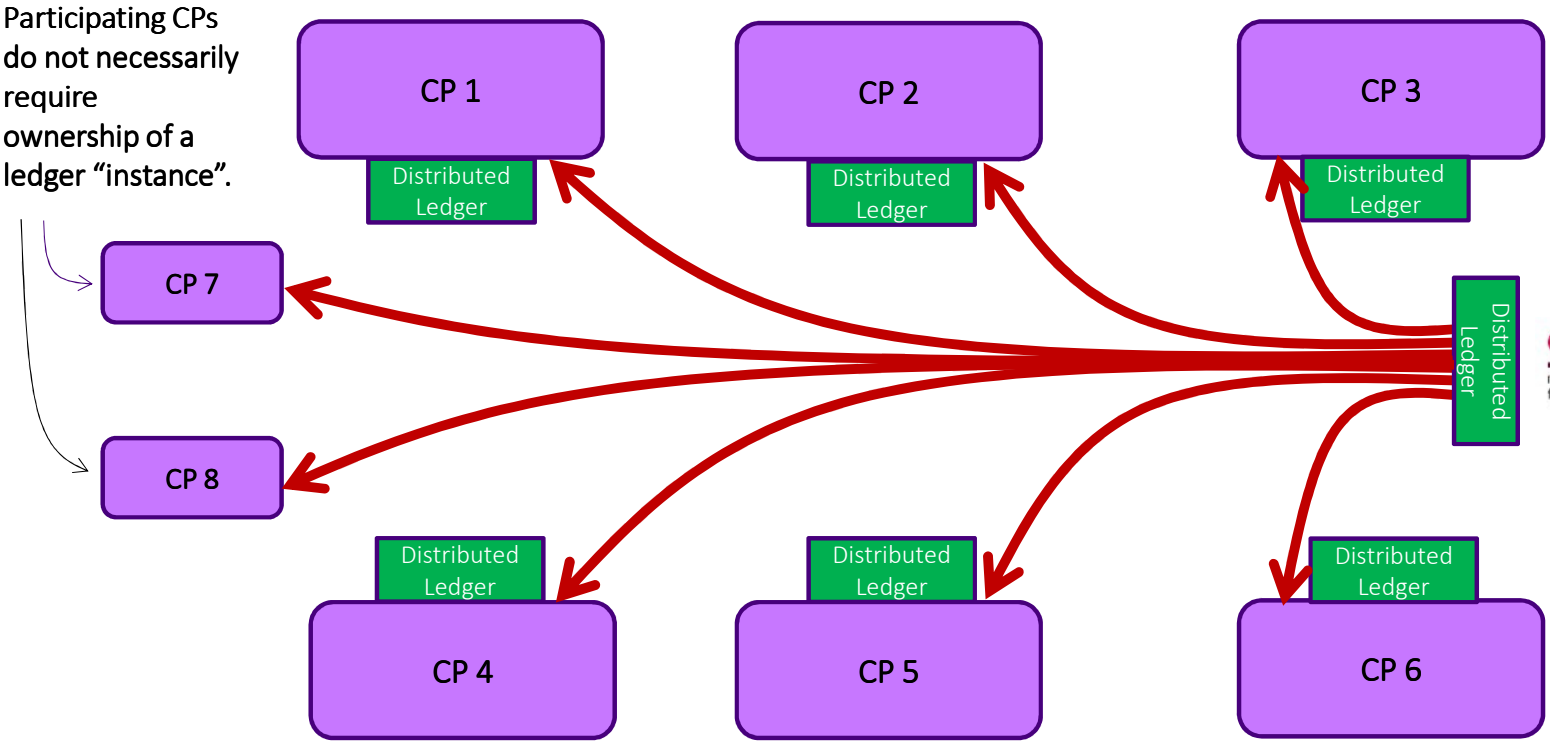
- The *Proof of Concept* uses open source *Linux Foundation Hyperledger Fabric* which has a modular architecture that is suited to the purpose and allows some of the consenus and participant membership characteristics of a solution to be implemented as “plug and play”.

- As the technology is evolving rapidly, alternatives such as Etherium and Corda, for example, will need to be evaluated in the event blockchain is the agreed way forward for a production architecture.

© British Telecommunications plc 2017

Blockchain PoC: “Permissioned” Participants

Participating CPs do not necessarily require ownership of a ledger “instance”.



Ofcom will assign and control CP access to the private blockchain consortium.

Ofcom
making communications work for everyone

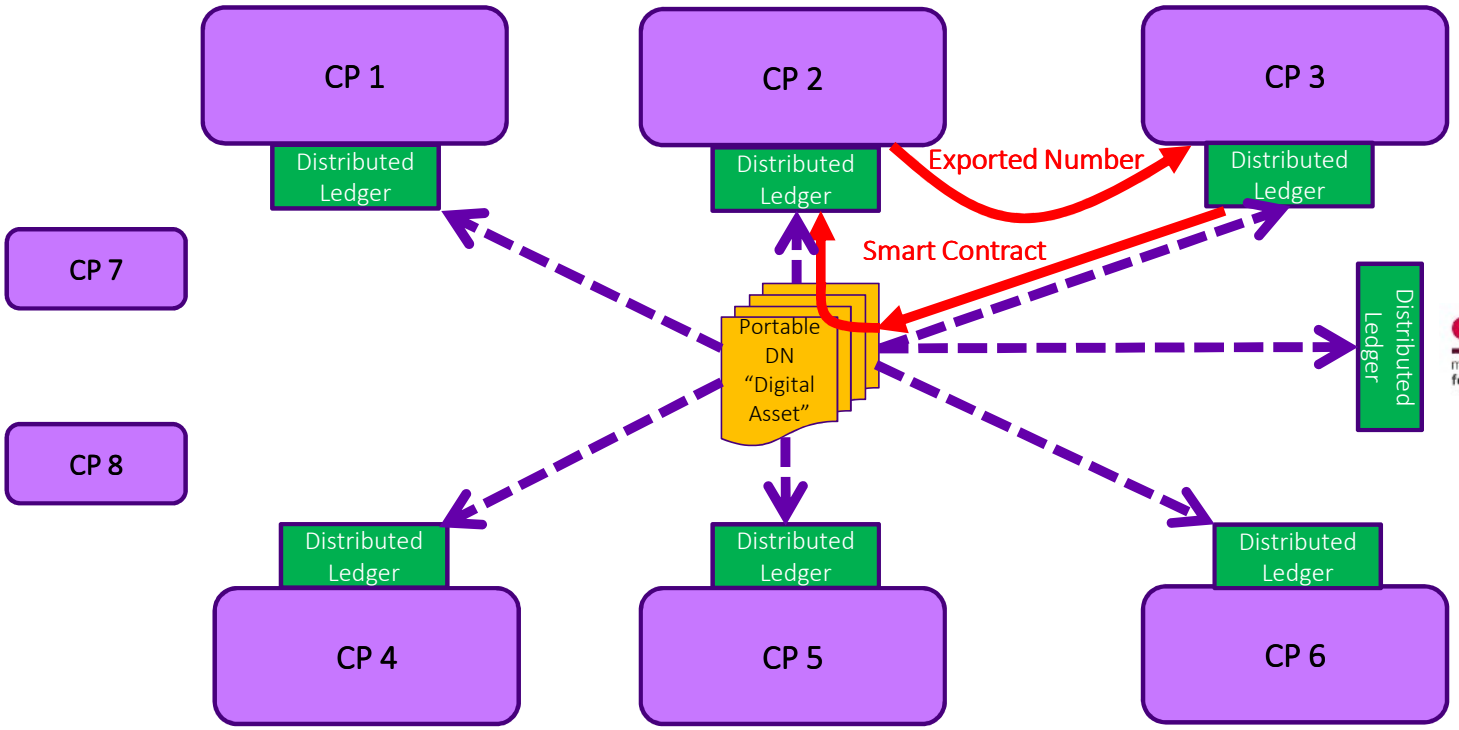
Steps:

1. Ofcom permits a CP to join the porting consortium.

© British Telecommunications plc 2018

BT

Blockchain PoC: Distributed Ledger



Ofcom
making communications work for everyone

Steps:

1. Ofcom permits a CP to join the porting consortium.
2. Raise the porting order and complete the export, updating the digital asset.
3. Distribute updates to each ledger instance via messaging.

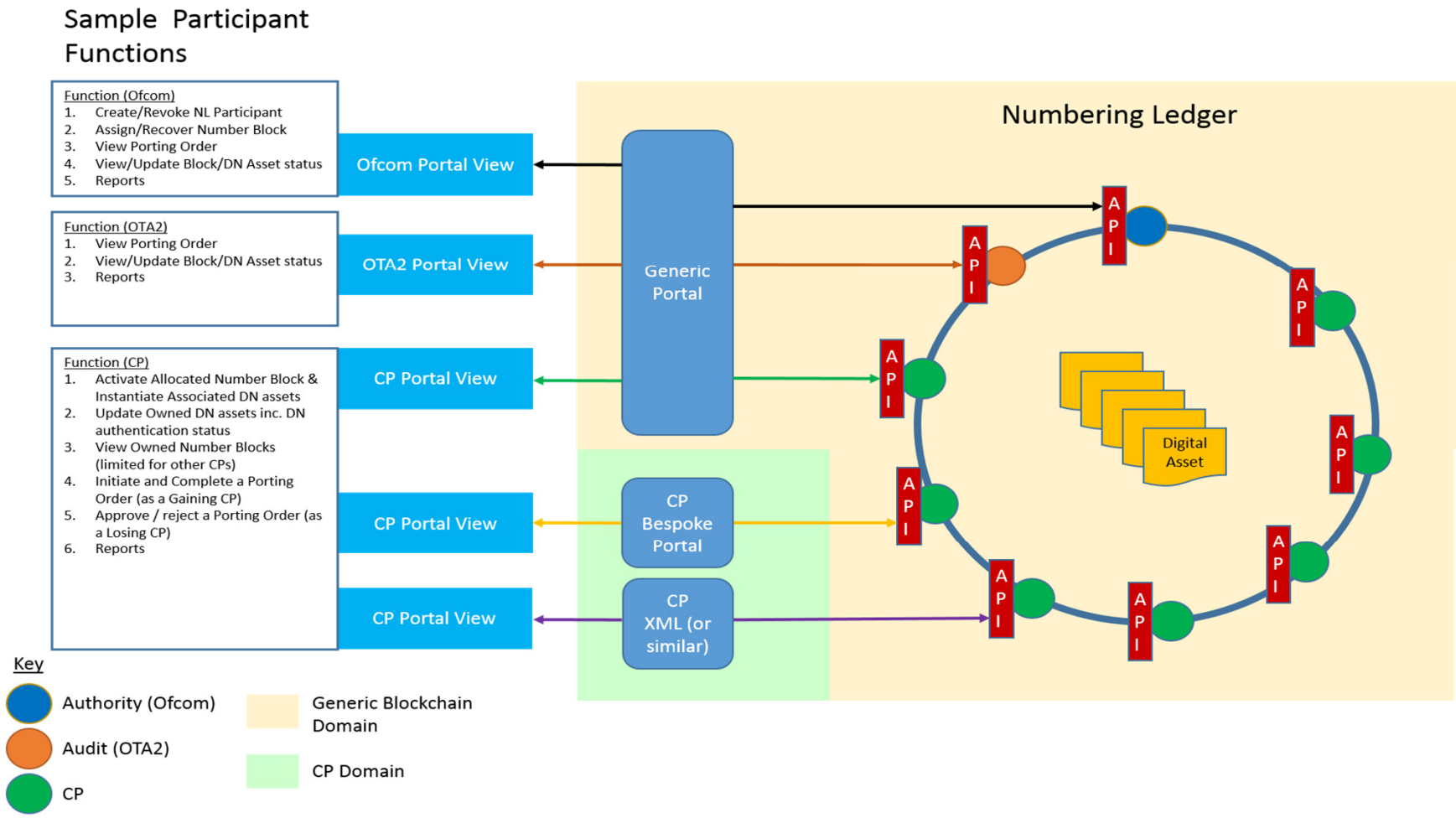
Example:

CP 3 imports a number from CP 2

© British Telecommunications plc 2018

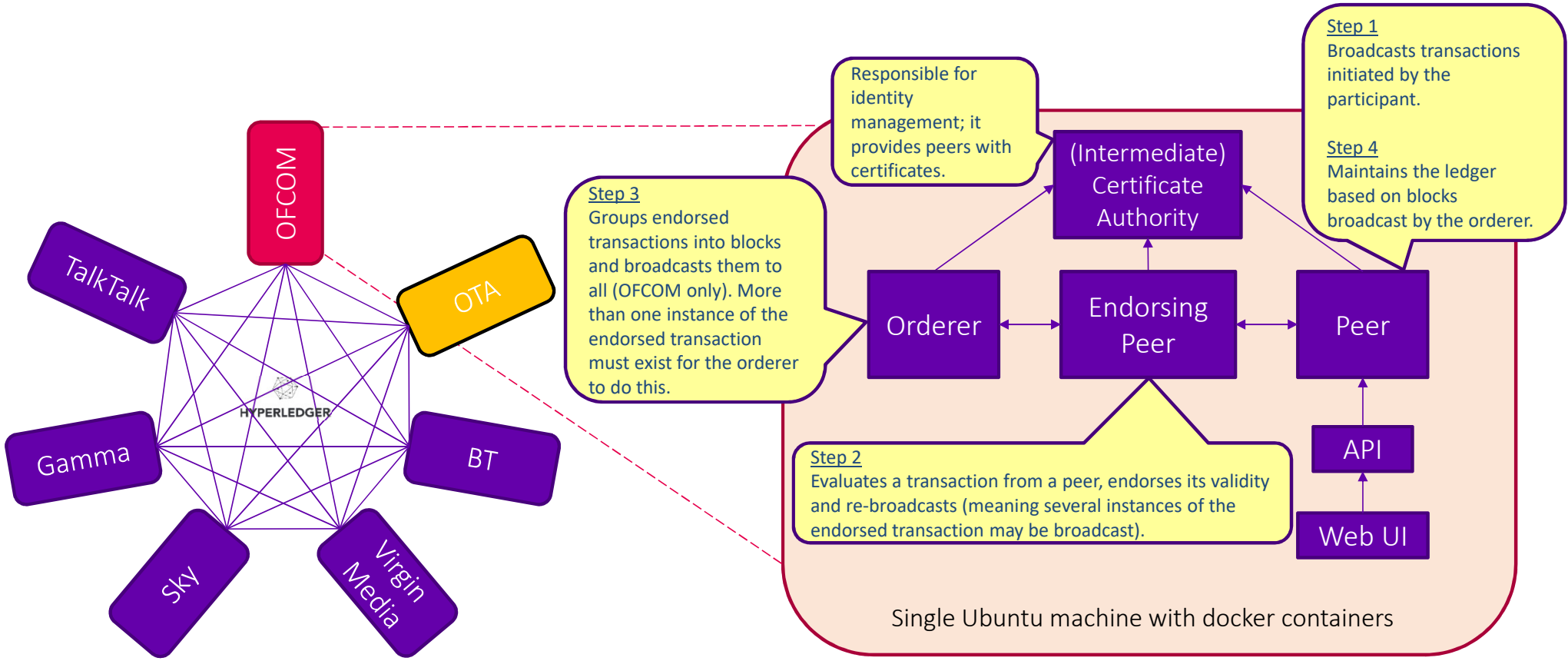
BT

Blockchain: Architecture Principles: APIs



PoC: Physical Architecture

Set-up



© British Telecommunications plc 2018

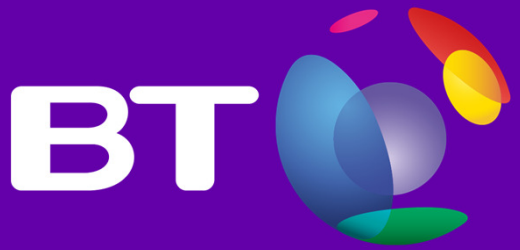
Further Investigative Work

Blockchain: Technical Evaluation

The *Proof of Concept* exercise will provide visibility and evidence that blockchain technology can be used and adapted to accommodate the proposed numbering use cases, but next steps will need to include further investigative work to build a more complete understanding of the technology and use case implementation. Some of these areas are as follows:

- Non-transactional Data Access & Download: the ability for a stakeholder to download ledgered digital asset data either in real-time or batched download, outside of a formal blockchain transaction between two parties, will be needed for different purposes e.g. to facilitate network switching updates for Direct Routing.
- Volume Messaging: updates to multiple assets may generate significant messaging traffic within a distributed architecture. We need to understand how to structure our data to minimise message generation and any constraints on message volumes and message payload size based on predicted demand.
- Other Non-functionals: the need for stress testing. The likely need to support approaching 1B number assets requires certainty that transaction and messaging volumes can be accommodated.
- Multiple asset updates per transaction: some scenarios will require update of multiple digital assets in context of a single transaction e.g. for a multi-number port order. The optimal approach to achieving this needs to be established.
- Restrictions on "Read" Data Access: blockchain is inherently based on a shared participant visibility of ledgered data. We need to better understand options for controlling read ledger access (both the assets that can be viewed and data attributes within an asset), based on a participant's role, although inherently, solutions will be designed on the shared visibility principle.

© British Telecommunications plc 2018


BT