



Combat Mobile Device Theft with blockchain-based Global IMEI Storage and Services Innovation

Benjamin Stöckhert, SAP
Krzysztof Sielski, Deutsche Telekom
Aseem Gaur & Andreas Göbel, Camelot ITLab

June 07, 2018

PUBLIC



SAP Blockchain Co-Innovation Program



Agenda

Blockchain in the Enterprise

Global IMEI Storage and Services Use Case

Demo

Q&A / Discussion

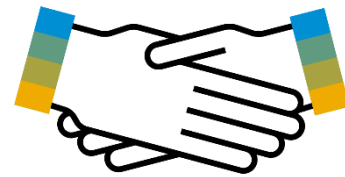
SAP Blockchain in the Enterprise



SAP's point of view: Blockchain Is....



Technology



**New networked-based
business models**



**Business
processes**

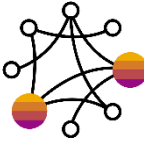
How to identify **Blockchain Use Cases?**



The need to share data



Multiple writers



Absence of trust

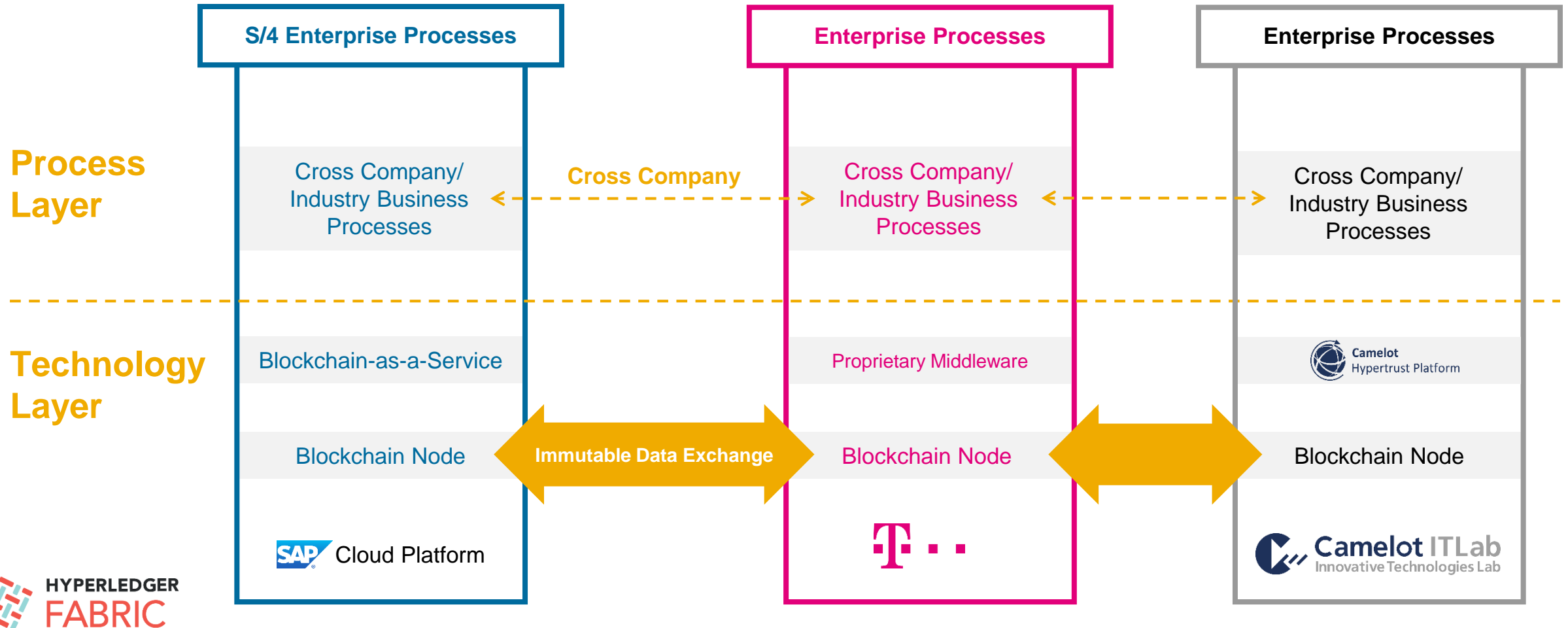


Disintermediation

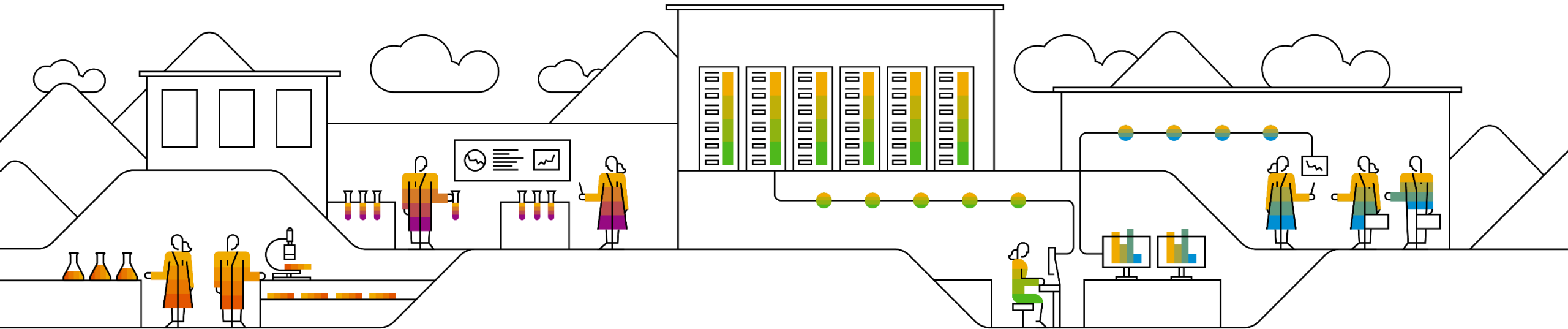


Transaction based interaction

Global IMEI Storage and Services High Level Architecture



Deutsche Telekom Global IMEI Storage and Services Use Case



Mobile Device Theft **On A Global Scale**

Each year, global mobile device thefts number in the millions



Mobile devices and the personal information stored on them are consistently among the highest priority targets for thieves throughout the world



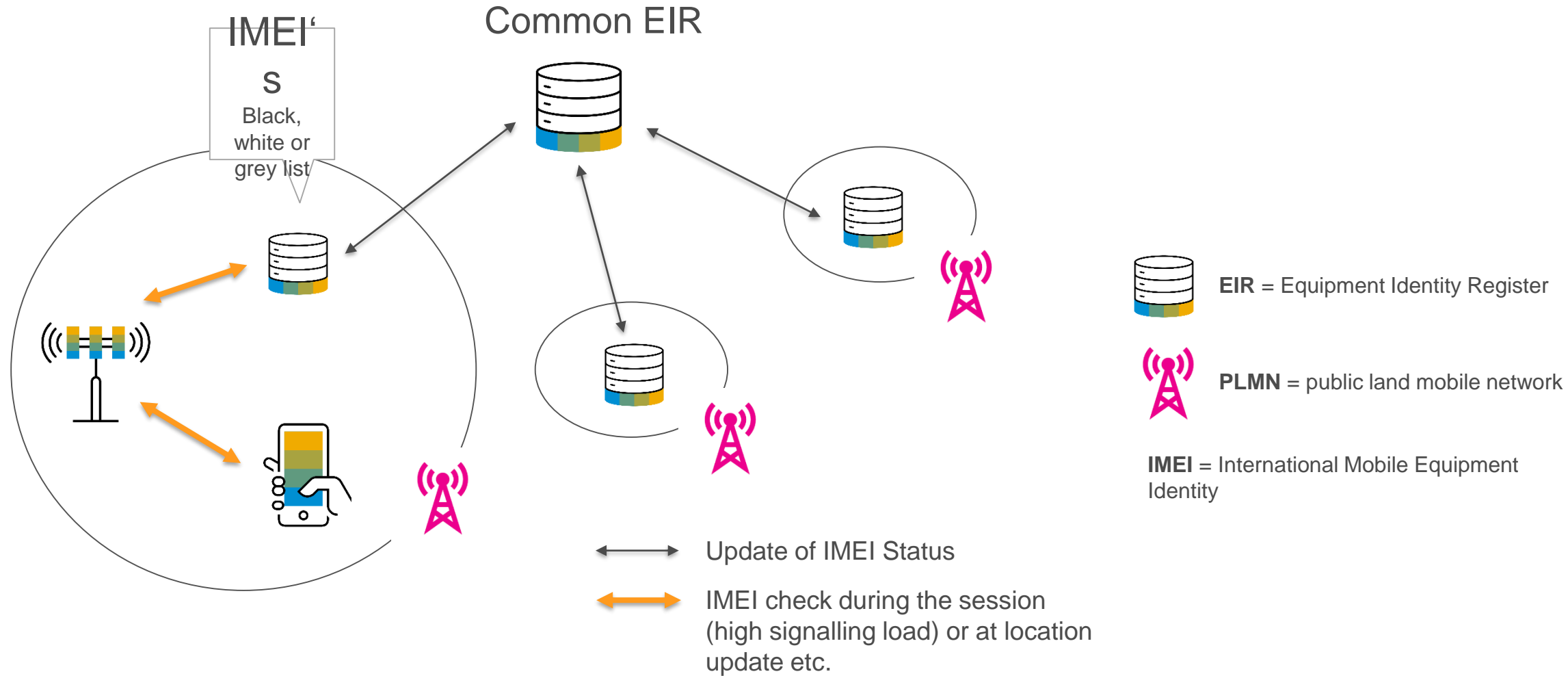
Studies estimate that by now, 1 in 10 smartphone owners in the US have been victims of phone theft in one form or another



IDG Research:

- 68% of phone theft victims are willing to put themselves in some amount of danger to retrieve a stolen device
- 10% report loss of confidential company data
- 9% had their identity stolen

Current Solution for Combating Device Theft



Benefits of IMEI Blacklisting



Reducing Phone Theft



Drying Out The Black Market



Securing Personal Information



Combating Identity And Insurance Fraud

Blockchain Technology for Global IMEI Storage and Services



Synchronized data sharing between participants



Consistent and reliable transactional infrastructure



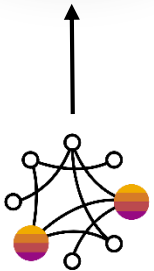
Blockchain-Based IMEI Blacklist



Administrative functionality for all members



Efficiency gains through break down data silos



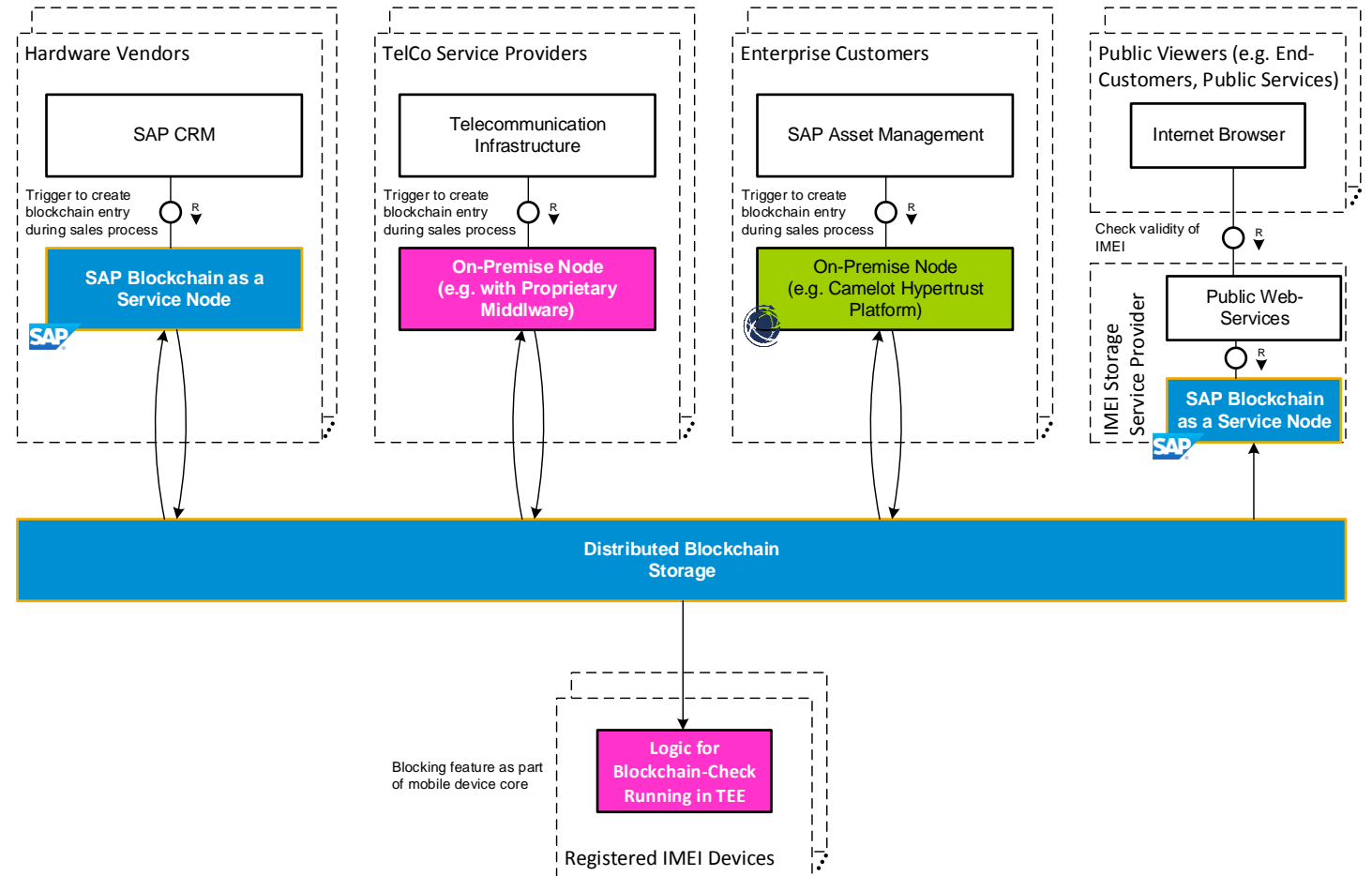
Transparency and mutually assured trust

Deutsche Telekom High Level Use Case

Blockchain-based IMEI Blacklist available to all participants



- Shared reality through the use of a distributed database
- Transparent and reliable transactions between participants
- Stream-lined and scalable blacklisting process



Camelot ITLab Demo



Questions & Answers



Thank you.



Benjamin Stoeckert

Business Development – Blockchain & DLT
SAP Innovation Center Network

SAP SE, Germany
M +49 151 18875315
benjamin.stoeckert@sap.com



Krzysztof Sielski

Partner Management TD GK
Business Solutions

Deutsche Telekom IT
M +49 1266 5482
krzysztof.sielski@t-systems.com



Andreas Goebel

Head of Center of Digital Innovation Blockchain
CC Cloud Architecture

Camelot ITLab
M +49 172 7810387
agob@camelot-itlab.com



Follow us



www.sap.com/contactsap

© 2018 SAP SE or an SAP affiliate company. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company.

The information contained herein may be changed without prior notice. Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

In particular, SAP SE or its affiliated companies have no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein. This document, or any related presentation, and SAP SE's or its affiliated companies' strategy and possible future developments, products, and/or platforms, directions, and functionality are all subject to change and may be changed by SAP SE or its affiliated companies at any time for any reason without notice. The information in this document is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, and they should not be relied upon in making purchasing decisions.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies.

See www.sap.com/corporate-en/legal/copyright/index.epx for additional trademark information and notices.

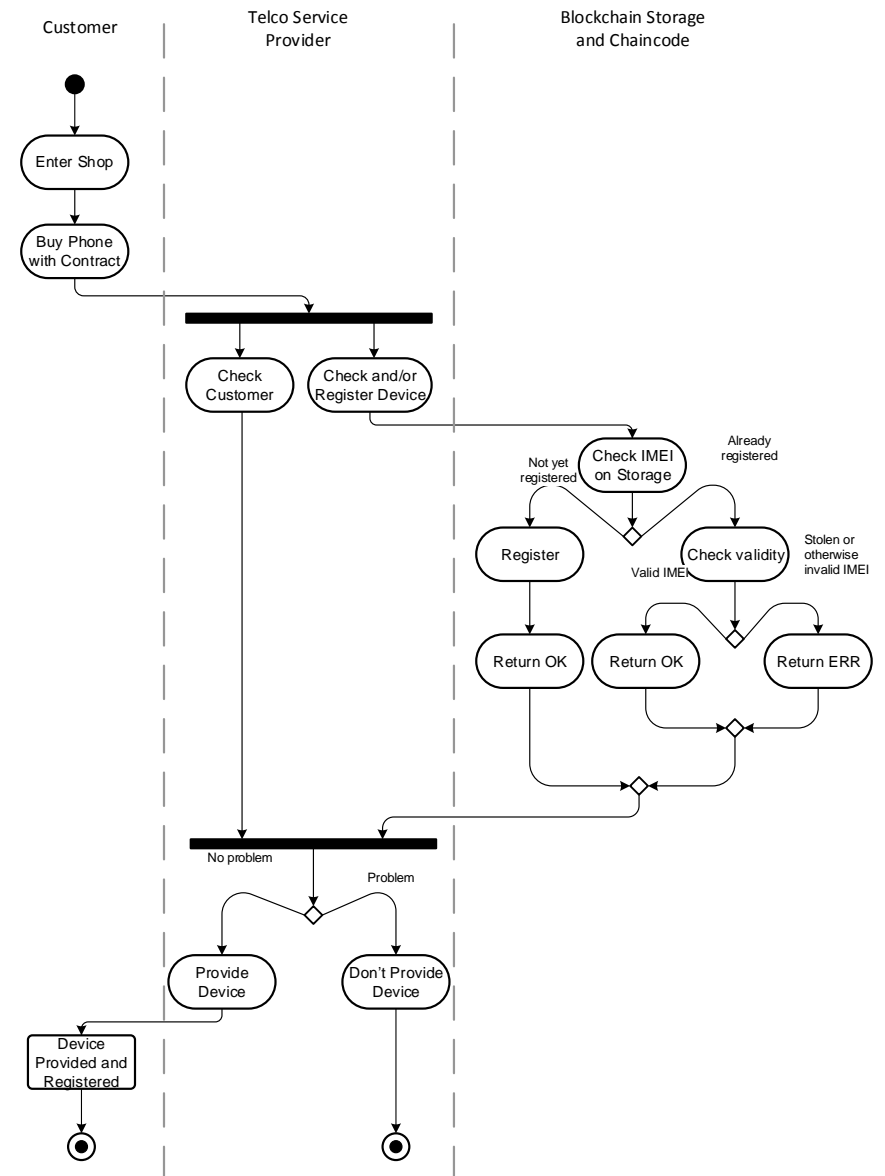
BackUp



Deutsche Telekom Use Case Example Sales Process

Using the **Global IMEI Storage Blockchain** to verify the prior supply chains during the sales process

Ensuring the **integrity of any purchase** conducted within the Telekom Stores



Deutsche Telekom Use Case **Example Network Services**

Using the **Global IMEI Storage Blockchain** to block compromised devices from accessing network functionalities of participating MNO's

Effectively allowing the targeted deactivation of **primary device functionalities**

