



SAP Innovation Awards 2019 Entry Pitch Deck

**Blockchain Accelerator for Mobile Device Management
Co-innovated with DTAG and SAP**

Camelot ITLab GmbH



<https://youtu.be/z-p7fdRJUcQ>

<https://youtu.be/3N39gPFKBZg>

Demand Generation via Press and Social Media

UPCOMING SPEAKING SLOT AT ASUG WITH SESSION NUMBER 84010

CAMELOT PRESS RELEASE



Camelot ITLab Introduces Blockchain Accelerator Package for Mobile Device Management

Monheim, 06/06/2018 - Camelot Innovative Technologies Lab (Camelot ITLab) today announced its Blockchain Accelerator for Mobile Device Management, powered by SAP Leonardo. The new solution helps end users and system administrators to manage mobile devices in a secure and efficient manner. It is a modular, scalable solution to protect mobile devices from data loss and unauthorized access. Based on SAP Leonardo technologies, the solution leverages the SAP Leonardo Mobile Management capabilities and offers new functionalities to mobile device management.

The new Camelot ITLab accelerator features a solution based on mobile phone and tablet devices and their users that is accessible to all operators, smart phone producers and system administrators. It is a modular, scalable solution to protect mobile devices in a secure and efficient manner. It is a modular, scalable solution to protect mobile devices from data loss and unauthorized access. Based on SAP Leonardo technologies, the solution leverages the SAP Leonardo Mobile Management capabilities and offers new functionalities to mobile device management.

<https://www.camelot-itlab.com/en/press/camelot-itlab-introduces-blockchain-accelerator-package-for-mobile-device-management/>

CAMELOT BLOG POST



Share on LinkedIn Share on Twitter Share on Facebook

'Camelot ITLab has developed a solution based on SAP Leonardo that makes it much easier to block stolen and lost smartphones. The first use case, which was implemented together with SAP and Deutsche Telekom, has already been reported on in the media. This blog post is about the underlying solution, the 'Blockchain Accelerator for Mobile Device Management'.

<https://blog.camelot-group.com/2018/12/using-blockchain-to-prevent-mobile-phone-theft/>

SAP NEWS



Die Deutsche Telekom, Camelot ITLab und SAP arbeiten an Blockchain-Netzwerken, um den Diebstahl von Mobiltelefonen zu verhindern. SAP und ITLab haben die größte Governance, die Blockchain-Netzwerke ausrichten, durch die Verknüpfung mit anderen kognitiven Fähigkeiten können auch technologische Innovationen entstehen.

<https://news.sap.com/germany/2018/06/deutsche-telekom-blockchain-smartphone-diebstahl/>

TELEKOM NEWS

Handy gestohlen? Telekom hilft mit Blockchain

- Deutsche Telekom erweitert Blockchain-basierte Technik für Sperrung gestohlener Handys
- Partnerschaft mit SAP und Cloud Platform Blockchain
- Dezentrale Speicherung für schnelle und unkomplizierte Geräteblockierung



<https://www.telekom.com/de/medien/medieninformationen/detail/handy-gestohlen-telekom-hilft-mit-blockchain-526596>

FORBES (USA)



<https://www.forbes.com/sites/sap/2018/10/18/deutsche-telekom-fights-smartphone-theft-with-blockchain/#44aebaa2c70>

MEDIUM (USA)

Deutsche Telekom Fights Smartphone Theft with Blockchain



<https://medium.com/sap-innovation-spotlight/deutsche-telekom-fights-smartphone-theft-with-blockchain-e5b9d48ac59>

COM-MAGAZIN

Datenschutz nach Diebstahl
Telekom testet Blockchain-basierte Smartphone-Sperrung



<https://www.com-magazin.de/news/blockchain/telekom-testet-blockchain-basierte-smartphone-sperrung-1544225.html>

E3ZINE



Camelot ITLab Introduces Blockchain Accelerator Package
2018-11-02 | Source: Camelot ITLab | in Blockchain, Press Release | Author: E3ZINE Magazine | Replies: 0
Camelot ITLab announced its Blockchain Accelerator for Mobile Device Management, powered by SAP Leonardo. The new solution helps end users and system administrators to manage mobile devices in a secure and efficient manner. It is a modular, scalable solution to protect mobile devices from data loss and unauthorized access. Based on SAP Leonardo technologies, the solution leverages the SAP Leonardo Mobile Management capabilities and offers new functionalities to mobile device management.

<https://e3zine.com/2018/11/02/camelot-blockchain-accelerator/>



Blockchain Accelerator for Mobile Device Management

Camelot ITLab (Medallion Partner) co-innovating with Deutsche Telekom

“Quote”

Blockchain is a disruptive technology with great potential. It was important for us to work with an expert consulting organization who has proven expertise in this field. Camelot and their blockchain-based Hypertrust Platform fully convinced us.

Hartmut Müller,
Senior Vice President Deutsche
Telekom IT GmbH

Challenge

Safeguard mobile devices and IoT devices in the event of loss or theft. Create an innovative International Mobile Equipment Identity (IMEI) blacklist solution (refer slide 4).

Solution

The accelerator provides the solution to end re-use of lost, stolen or invalid mobile devices: A blockchain based list of serial numbers and their owners, that is accessible to all manufactures, operators, OEM's and other players to increase trust and data security for all stakeholders.

Outcome

Blockchain based solution to prevent theft
Enhancement to SAP Blockchain as a Service – on-prem nodes, first PoC with Deutsche Telekom
Demand Generation via Press / Social Media coverage

Refer Slide 6

Camelot Blockchain Accelerator for Mobile Device Management



AUTHENTICATION OF DEVICES VIA BLOCKCHAIN

The accelerator provides the solution to end re-use of lost, stolen or invalid mobile devices: A blockchain based list of serial numbers and their owners, that is accessible to all manufactures, operators, OEM's and other players to increase trust and data security for all stakeholders.



INDUSTRY OPERATION

- ▶ Sharing blacklist across operators, manufacturers and other agencies
- ▶ Access control of business customers via SAP system
- ▶ One stop SAP blockchain solution for tracking devices (lost/stolen)
- ▶ Device validation before and after the booting process



BUSINESS CHALLENGE

- ▶ Information on stolen devices is kept in local database of a given Mobile Network Operator (MNO)
- ▶ Limited & expensive information exchange between various stakeholders
- ▶ No available solution to protect property of mobile equipment vendors within their supply chain or prior to sale of the device to the end customer by a given MNO
- ▶ In case a device is lost or stolen separate interaction with each MNO is required



Business Benefits

Loyalty & Trust

- ▶ Only information which needs to be shared by the parties is shared in the blockchain
- ▶ Local storage of information

Data Protection in Case of Theft

- ▶ Block/Kill switch to protect the data on the device in case of loss or theft
- ▶ In case a device is lost or stolen, the customer has to interact with each MNO separately

Transparency & Security

- ▶ Information on blockchain is inalterable
- ▶ Storage of ownership information for mobile devices – for mobile phones connected to IMEI (International Mobile Equipment Identity) as well as for devices in context of IoT



Customer Satisfaction

- ▶ Value added services for enhanced customer experience
- ▶ Mobile device check on eCommerce platforms
- ▶ Protection of credit card information and other sensitive data in case a mobile device got lost or stolen

Ease of Tracking Information

- ▶ Sharing a blockchain based blacklist across operators, manufacturers and other stakeholders
- ▶ Simplify identification of stolen devices
- ▶ Possibility of ending their usage – safely and in real-time



Partner Information

Deutsche Telekom AG Co-Innovation Partner



The re-use of stolen smart phones is a serious issue for both network operators and device producers. However, above all, corporate or private end customers arguably suffer the most. With our new blockchain accelerator package, we provide a solution tailored to the needs of these stakeholders.

Aseem Gaur,
Chief Leonardo Officer Camelot



Business Challenge & Objectives

- Refer Slide 5
 - Information on stolen devices is kept in local database of a given Mobile Network Operator (MNO)
 - Limited & expensive information exchange between various stakeholders
 - No available solution to protect property of mobile equipment vendors within their supply chain or prior to sale of the device to the end customer by a given MNO
 - In case a device is lost or stolen separate interaction with each MNO is required
-
- Sharing blacklist across operators, manufacturers and other agencies
 - Access control of business customers via SAP system
 - One stop SAP blockchain solution for tracking devices (lost/stolen)
 - Device validation before and after the booting process



Project / Use Case Details

A vendor of mobile phones is connected to the Blockchain for Mobile Devices Management system. It will register the IMEI numbers of all produced devices through the service. Through a public key infrastructure (PKI), the integrity of the data and the authenticity of the vendor is guaranteed. At the same time, the vendor is recorded as the OWNER and the GUARDIAN (guardianship is currently needed for the sake of end-user experience) of the item uniquely identified through its IMEI number.

As a next step in the process of device disposal, the registered mobile phones will be sold to telephone companies (telcos) or resellers. During the sales process, the OWNERSHIP of the device will be handed over to the telco (or reseller). This step can ONLY be triggered by the current owner (the vendor in this case), through PKI features. The GUARDIANSHIP, though, will still be kept by the vendor, for additional fallback actionability.

As a next step in the process of device disposal, the mobile phones will be sold to end customers (private entities). During the sales process, the OWNERSHIP of the device will be handed over to the private entity. Status quo the private entity does not have access to the Blockchain for Mobile Device Management network and so cannot participate in the PKI (shall be changed on the long run). So, the telco or reseller takes over the role of the GUARDIAN.

The case of theft:

The owner (private entity) calls the guardian (telco or reseller), is authenticated with the already available measures (address comparison or similar) and the device is locked by the guardian on the blockchain.

Result: The phone can no longer be used to make calls through the telco infrastructure and is not even able to connect to the internet via wifi (if a TEE implementation is on place on the device). The device is basically no longer usable.

The case of reselling:

The current owner informs the guardian, that the ownership shall be changed to another private entity. This change will be done by the guardian. A guardianship change can be involved here, too, e.g. in case of a telco switch. This can be also a use-case for additional service providers using the Blockchain for Mobile Device Management (integrated e.g. on marketplaces like Ebay etc.).

On the long run, private entities shall be enabled to trigger this process on their own (e.g. by providing a public key for the PKI during the sales process).



Benefits and Outcomes

Business / Social

Ease of Tracking Information

- Sharing a blockchain based blacklist across operators, manufacturers and other stakeholders
- Simplify identification of stolen devices
- Possibility of ending their usage and ownership change

Customer Satisfaction

- Value added services for enhanced customer experience
- Mobile device check on eCommerce platforms
- Protection of credit card information and other sensitive data in case a mobile device got lost or stolen

IT

Transparency and Security

- Information on blockchain is inalterable
- Storage of ownership information for mobile devices – for mobile phones connected to IMEI as well as for devices in context of IoT
- Information on blockchain is inalterable

Human Empowerment

Data Protection in case of Theft

- Block/Kill switch to protect the data on the device in case of loss or theft
- In case a device is lost or stolen, the customer has to interact with each MNO separately

Loyalty and Trust

- Only information which needs to be shared by the parties is shared in the blockchain
- Local storage of information



SAP SE hereby confirms that the Camelot ITLab Blockchain for Mobile Device Management accelerator powered by SAP Leonardo of the company Camelot ITLab GmbH has been certified to meet the best practices of an industry accelerator powered by SAP Leonardo.

The certification test for Camelot ITLab Blockchain for Mobile Device Management v1.0 is documented in report no. 12402 on May 24th, 2018 and expires on May 24th, 2019.

SAP LEONARDO TECHNOLOGY USED:

SAP Leonardo Analytics
SAP Leonardo Blockchain

For component details please review the test report.

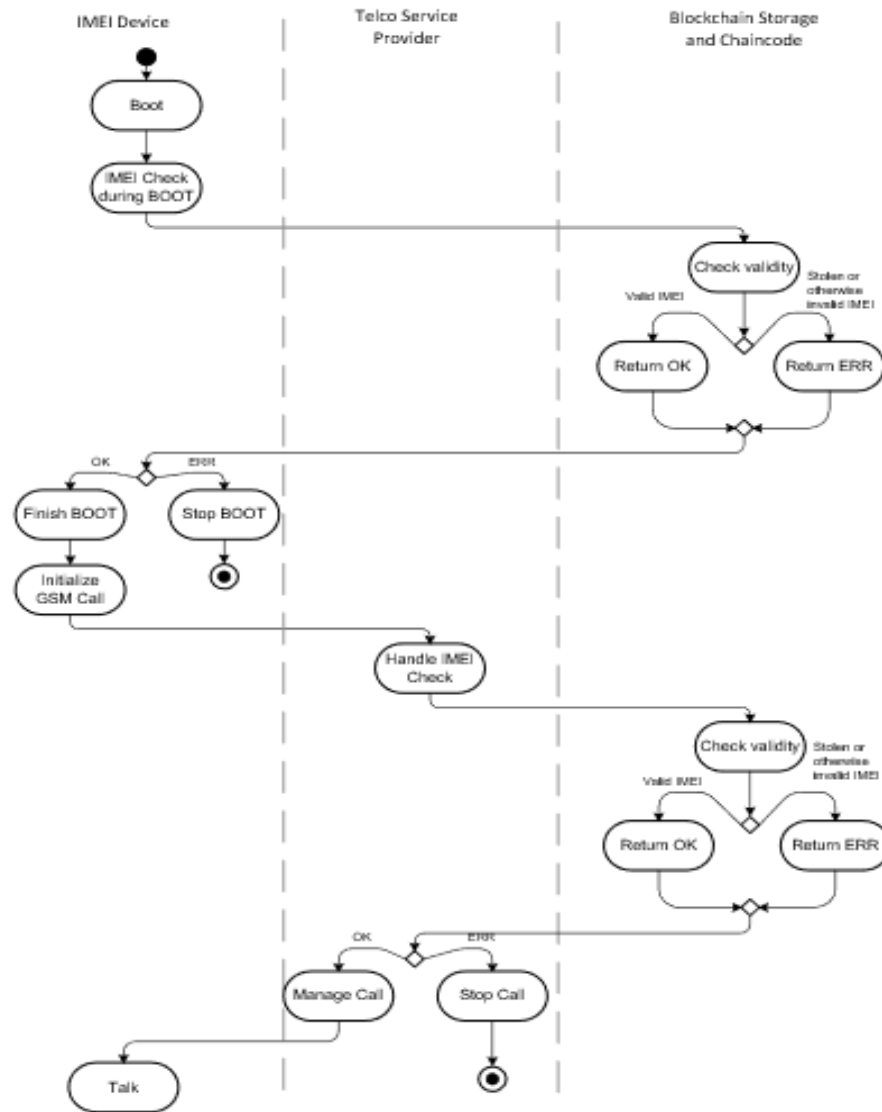
This certificate confirms the readiness of features in accordance with SAP certification procedures as outlined in the scenario for SAP Leonardo Industry Accelerators (LEONARDO-ACC 1.0). It does not guarantee that the industry accelerator is error-free.

Montreal, May 24, 2018

Angela Yip, SAP Labs Canada



Architecture





Deployment

Date of Deployment or POC: 23.05.2018

Number of live users: 10



COSTS

CAMELOT: Approx. € 60 K

USAGE 6 MONTHS



Accelerator includes or requires (SAP BoM):

- ▶ SAP Cloud Platform Blockchain Service Node: 8005564, 8006078
- ▶ SAP Fiori: 8004509, 8004508, 8004019
- ▶ SAP Analytics Cloud: 8004099, 8004100

Accelerator includes or requires:

CAMELOT Hypertrust Platform (6 months)



FEATURES INCLUDED

- Blockchain Introduction ✓
- Blockchain Network with 3 Nodes ✓
- Mobile or IoT Device Registration ✓
- Status & Usage Reporting ✓
- Ownership Change ✓
- Guardianship Token System ✓
- End User Token System ✓



Emerging Technologies and Use Cases

The following Emerging Technologies and use-cases are part of the project and describe the contribution

	Technology or Use Case	Yes/No	Contribution to Project
1.	Machine Learning / Artificial Intelligence	NO	
2.	IoT	YES	IoT is used to track the devices
3.	3D printing	NO	
4.	Blockchain	YES	Blockchain is used for the data storage and unifies all involved parties of mobile device management.
5.	API Economy / Integrate the Intelligent Enterprise	NO	
6.	Cloud Native / Event Based Architectures	NO	
7.	Extending the digital core with SAP CP / ABAP in SAP CP	NO	
8.	SAP Leonardo Application (extending SAP application, using Industry Innovation Kits or result of Design Thinking workshop)	YES	Creation of first Leonardo Blockchain accelerator in collaboration with Deutsche Telekom and SAP.

Short implementation period and predefined key activities enable on demand business benefits

