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

Abstract:
Each mobile device has its unique IMEI (International Mobile Equipment Identity) number that can be used to identify the device in a mobile network and to steer actions related to a specific device. For example, if the device was reported as stolen, mobile operators have measures to blacklist a given device from registering to and using their network. Even if a SIM card would be replaced in a stolen device (and SIM card related phone number would change) the device will not be able to use the network of the given operator as the blacklists are arranged around these device specific IMEI numbers. This solution however is limited to the operator's local blacklist and a mechanism to exchange information from the blacklist globally, among all operators is needed. There where efforts within GSMA - the organization that gathers all operators - to introduce common blacklist and a mechanism to share and exchange this information. The solution is not widely used in the mobile networks mostly due to the cost reasons. In some countries, a corresponding regulation was introduced and theft of mobile devices has been reduced on a national level but a global solution with wide acceptance is still to be seen.

Thanks to its distributed nature blockchain technology provides an innovative platform for solution around IMEI blacklist. Operators could participate in the blockchain network, store information about stolen devices and share it with other participants of the network. Advantage of this approach, in comparison to former efforts, is that such network could be open to accept other participants on top of mobile operators and in this way, generate extra stimulus and incentives to deploy the solution globally.

For the moment, the information about blacklisted devices is used only within processes on the network-side. Opening of access to this information could provide basis for new, complimentary solutions and mechanisms build e.g. on the device-side (blocking of connectivity directly on the device, deletion of sensitive data, reporting device location to enable tracking, etc.). In the same manner, the maintenance of the information stored on blacklist is today done solely by the operators. The blockchain based solution - given that corresponding permissions would be granted - could allow direct integration for example others for Asset Management systems. Such integration would provide aims e.g. to corporate customers to directly manage information about devices used by their employees (or any mobile or IoT device being owned by such company) on their own.

Additionally, further services or products could be build. Some examples would be:
- access for public authorities like police to verify device ownership and status of a device,
- products for the insurance industry where verifiable information about theft is relevant,
- services to provide ownership/status information on devices being traded on the second-hand market

and many more.

As a next phase, a natural extension of the solution would be to cover not only mobile phones and IoT devices where IMEI is unambiguously identifying the device but also other devices wherever analogous identifiers could be used (e.g. MAC addresses for laptops, tablets, etc.)

Putting the IMEI blacklists on blockchain could improve today's solution immediately. It would be a first step towards an ecosystem of participants and services that could be build around this solution and where full potential can be achieved only thanks to enablers like blockchain.