Identity Management in IoT Networks Using Blockchain and Smart Contracts

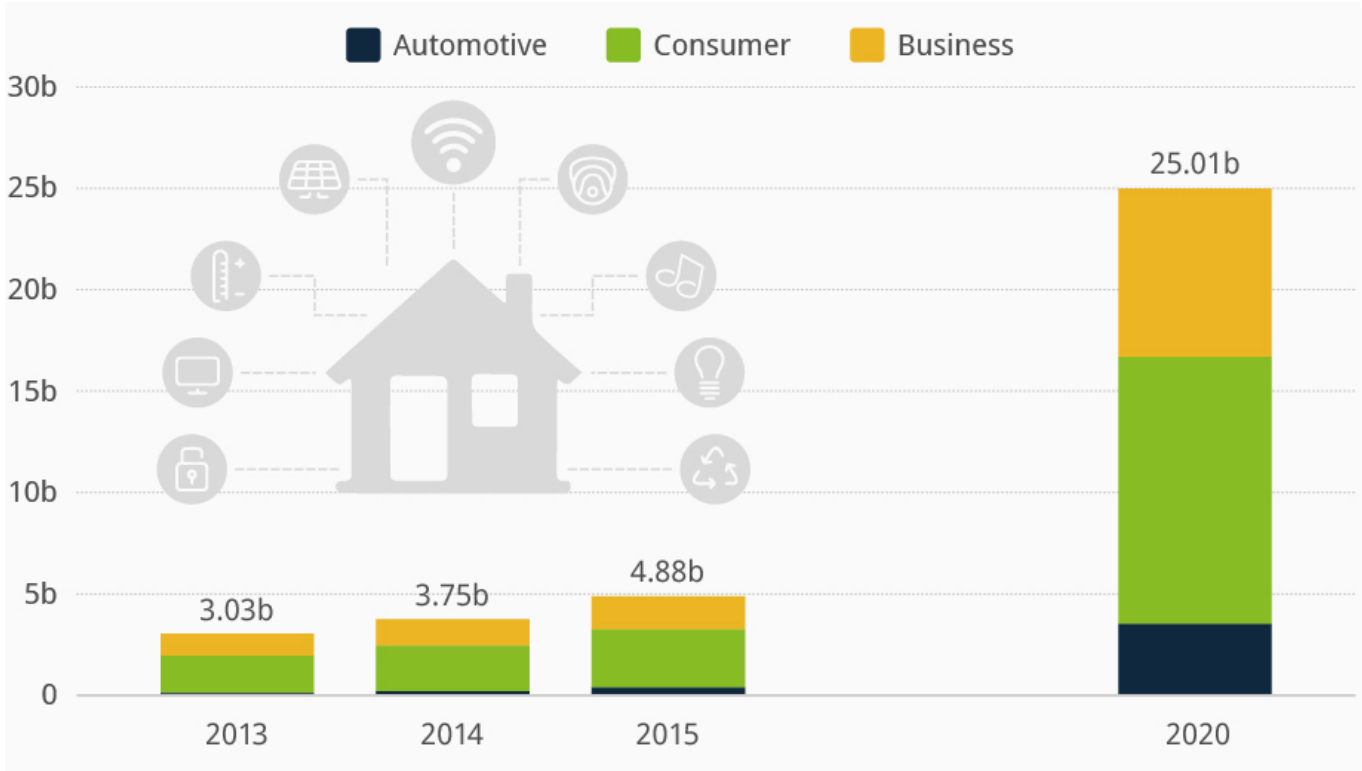
Authors: Ahmad Sghaier Omar
Electrical and Computer engineering Dept
University of Waterloo, ON, Canada

Outline

- Device Identity in IoT
- Identity Model and Life Cycle.
- Blockchain for Identity Management.
- Implementation Details.
- Use Case Smart Phone Anti-Counterfeiting.
- Conclusion.

IoT Adoption and Industry Figures

- The number of connected devices has surpassed 7 billion devices in 2017, and insights foresee a number of 20-25 billion connections by year 2020

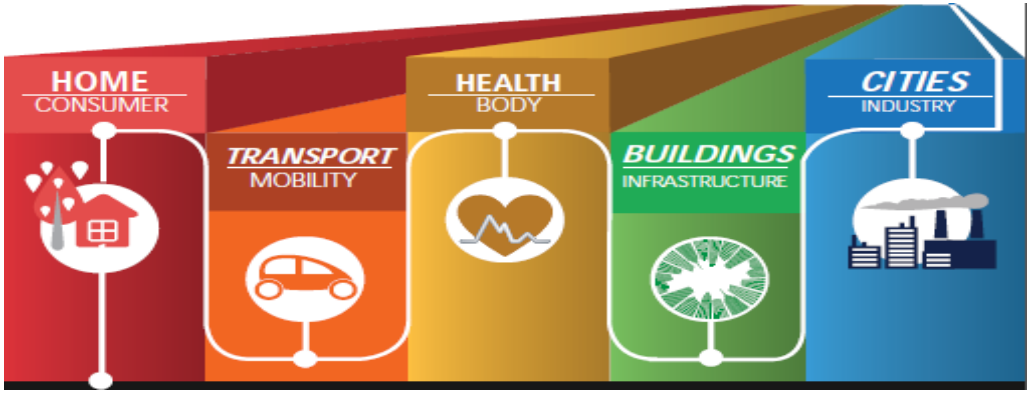


Gartner Symposium/ITxpo in November 2015

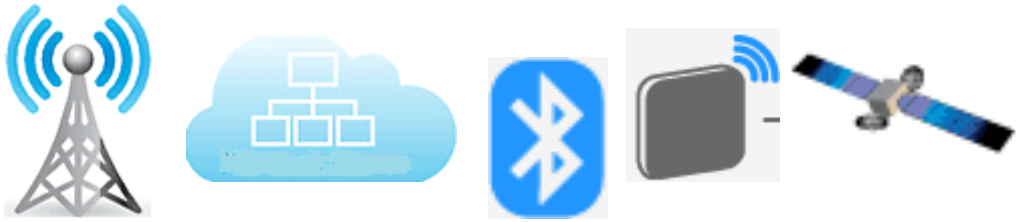
The IoT requires strong device identity and Root of Trust at its foundation

Heterogeneity

Services and Applications



Network



Devices and Sensors

Interaction

Communication

IoT Devices Identity Challenges

Heterogeneity

Unique & Global Identification

Centralization

P2P Applications

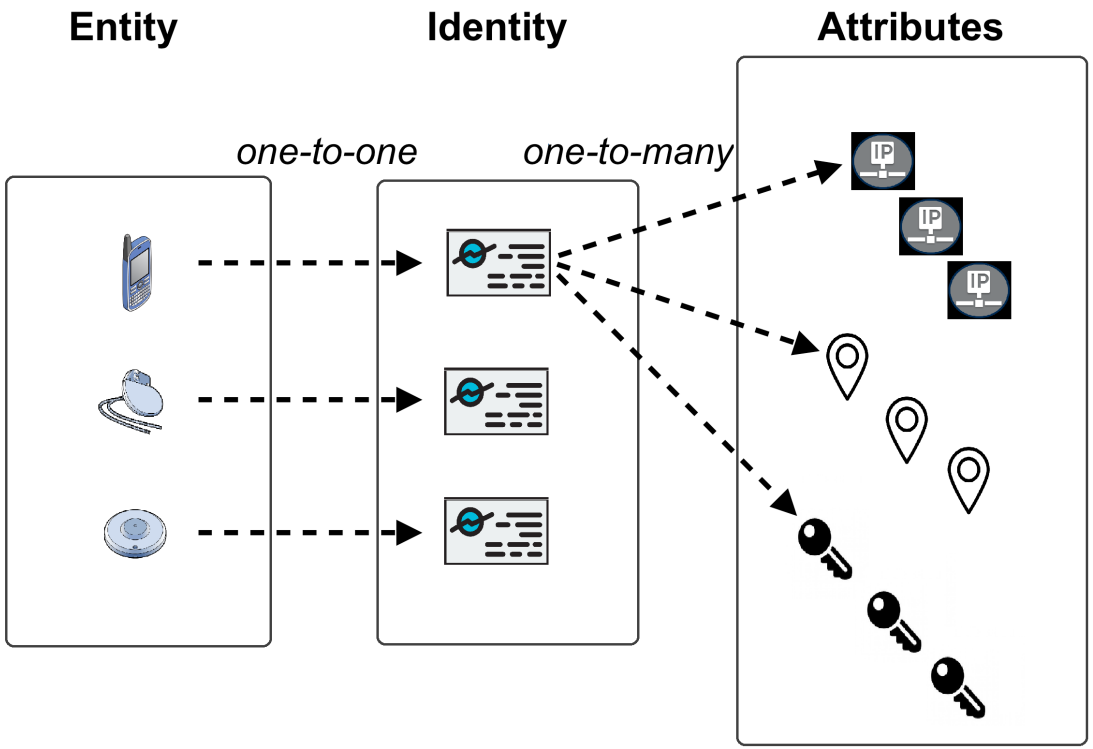
End-2-End

Authn/Authz & Access Control

Device Identity Relationship Model

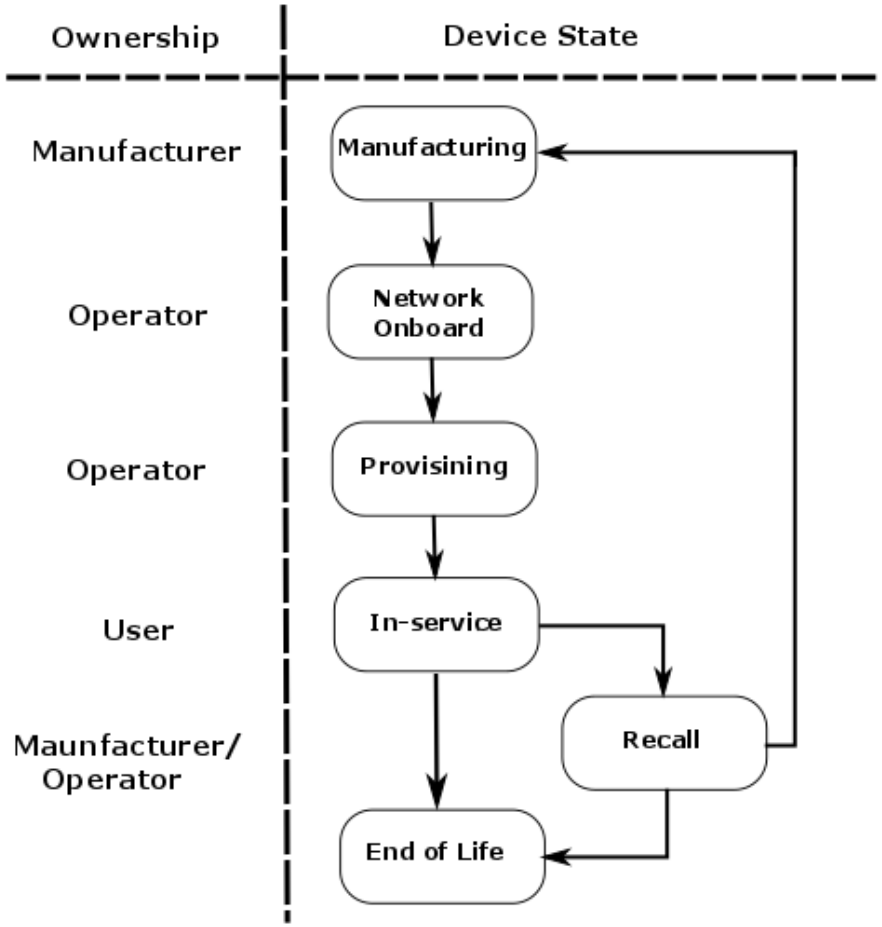
- Identity is a living asset, a device is given its identity at birth (e.g. manufacturing).
- An identity is the ”set of attributes related to an entity”.
- The device maintains its identity with updates and versions as pre-defined changes happen.

$$E_i \Leftarrow ID_i \Leftarrow < A_{i1}, A_{i2}, , A_{in} >$$



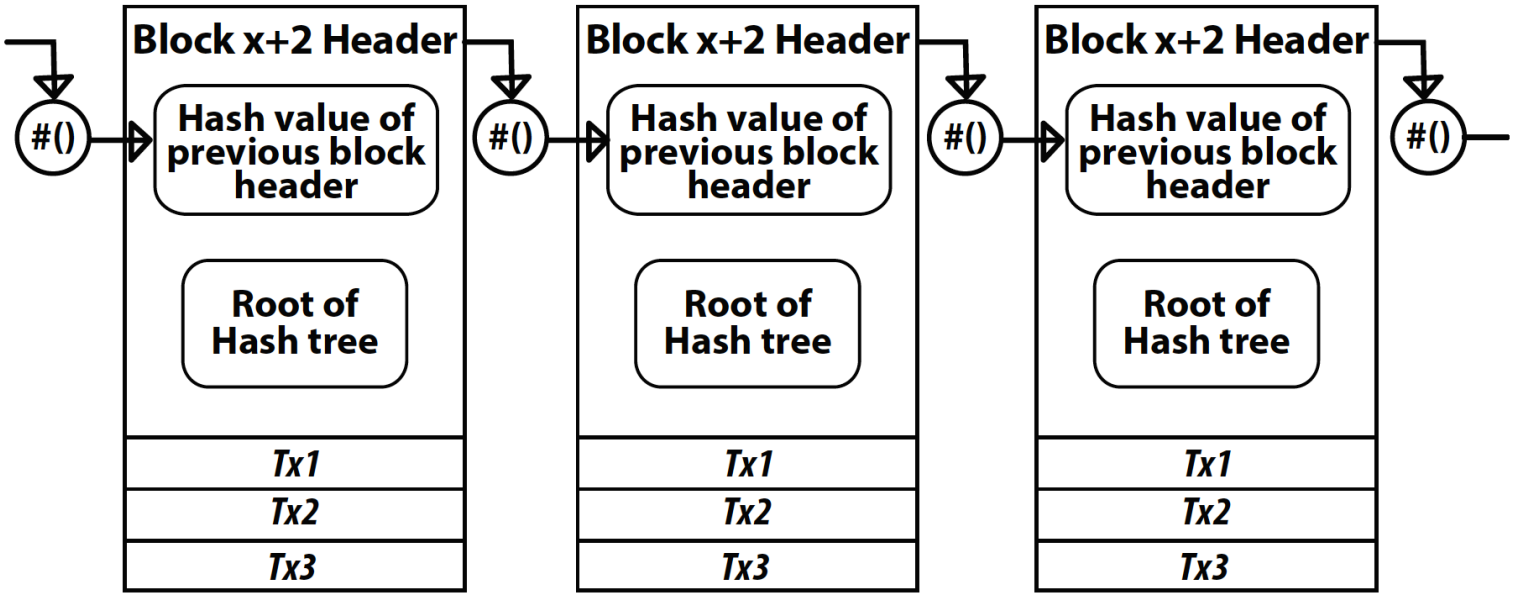
Device Life Cycle

- In IoT networks, devices go through a life cycle
- The IdM defines the device status and its ownership.
- The identity as a living asset should be maintained and updated, where a new version if required is issued as the devices owner changes or the device status on the network changes.



A fit for DID

- Immutable records
- Traceability
- Provenance
- Cryptographic Identifiers.



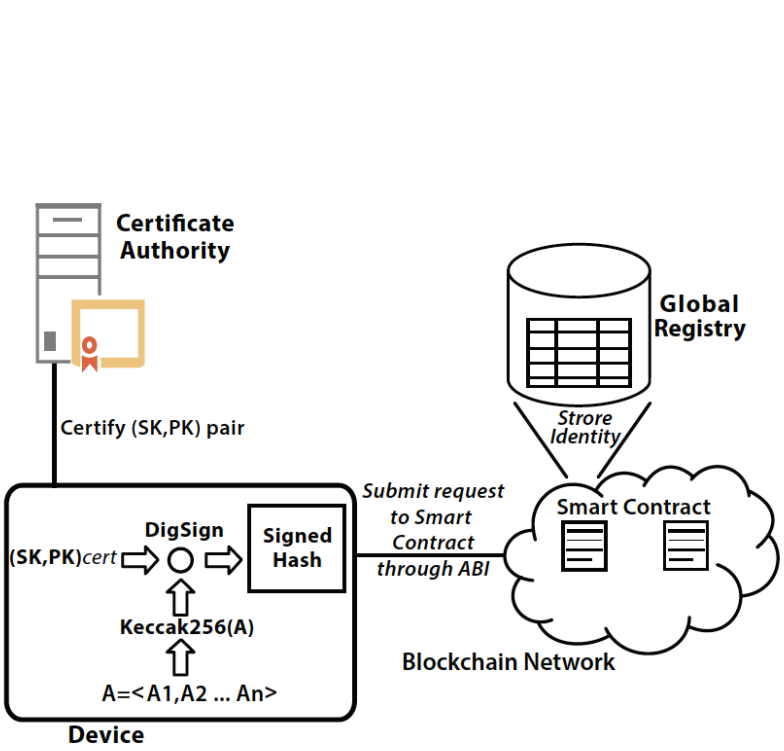
DID Fields

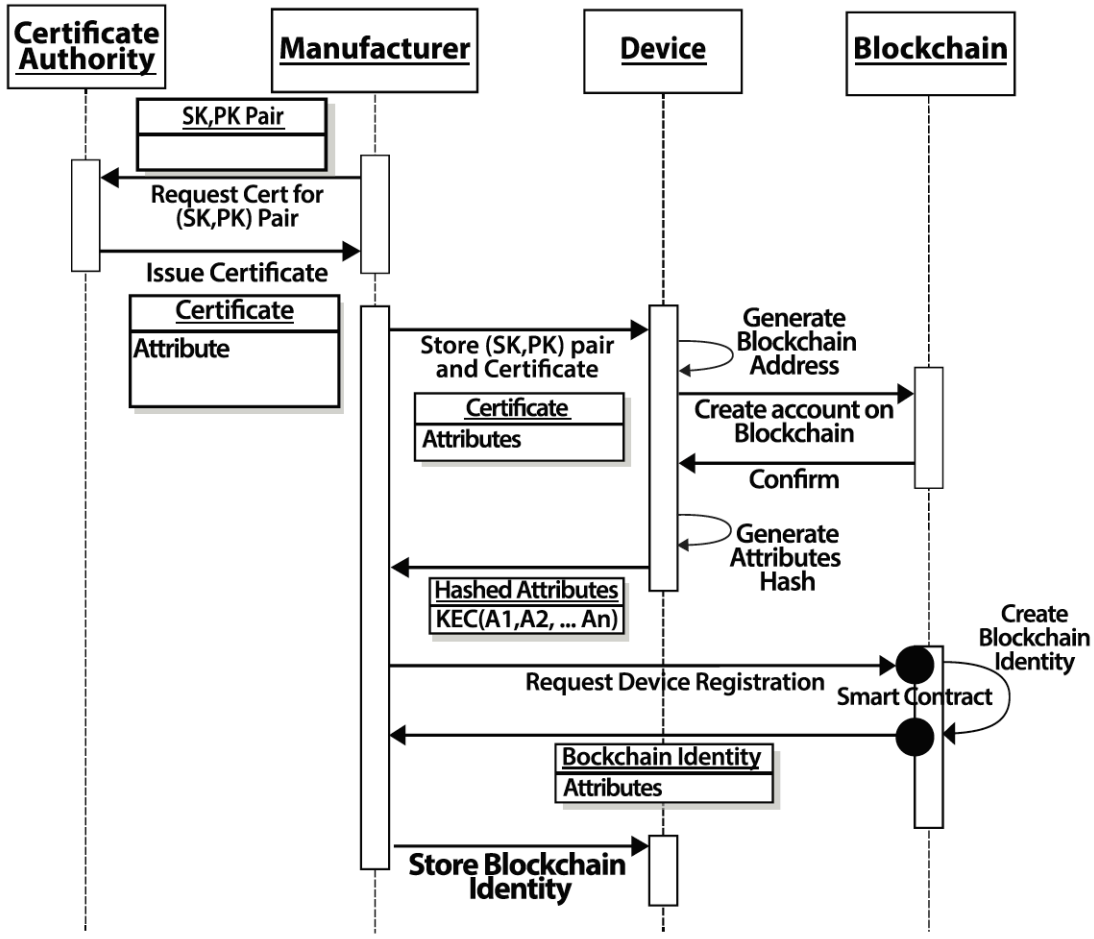
- Cross-ownership and Assignement
- Ownership Tracing
- Ubiquity and Uniqueness
- Portability (BYODID)

DIGITAL IDENTITY DATA STRUCTURE.

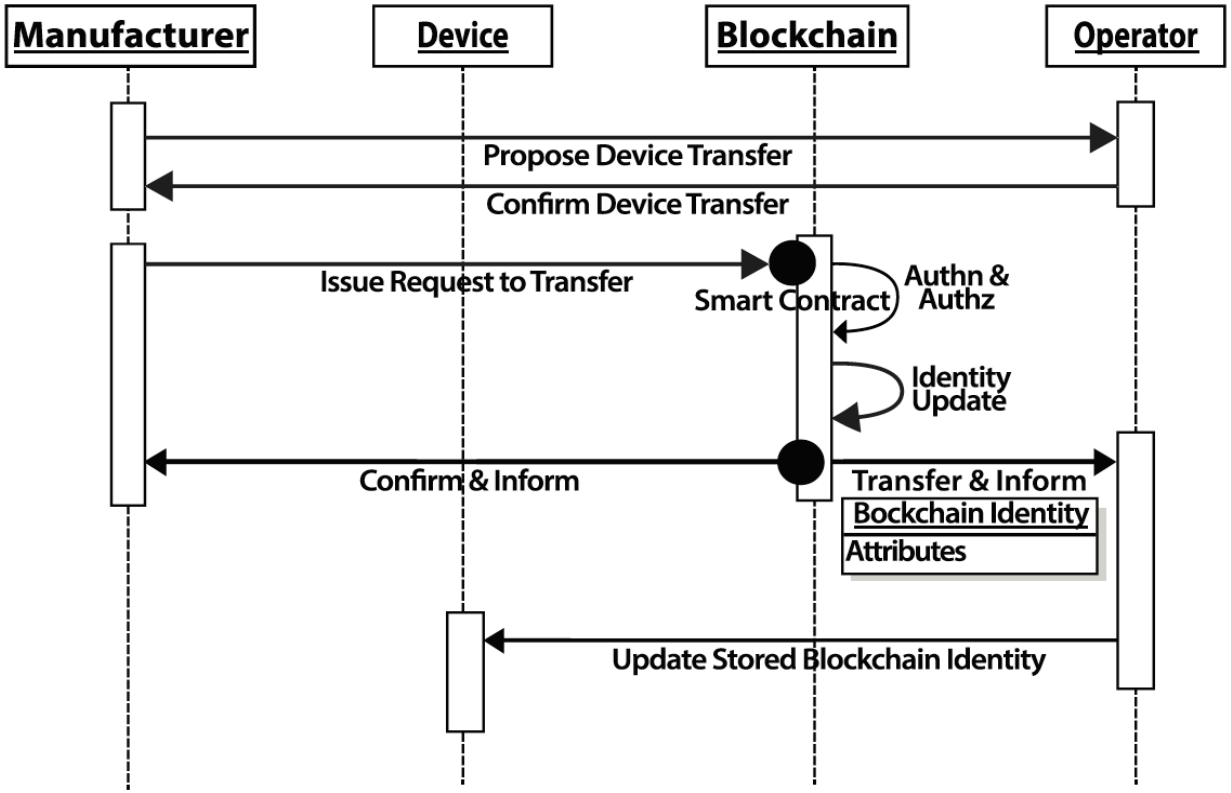
Field	Description
Device Address	The Ethereum address generated and assigned to the IoT device.
Owner Address	The Etheruem address assigned to the IoT device owner.
Attributes Hash	The result of hashing function of certain attributes of the IoT device such as MAC address, serial number ... etc.
First Block	The Block number at the time of creating the identity.
Last Block	The Block number at the last time of updating the identity.
ID Revision	An incremental number of the latest revision of the identity.
Identity Flags	A set of flags to identify certain features such as is the identity updatable, is it revocable, is it transferable.

Device Identity Creation





Device Identity Transfer of Ownership.



Smart Contract Global Registry

Algorithm 1 Contract global_registry

Require: *main registrar address*

```
public address main_registrar;
public struct {
    address assignee_address,
    String assignee_details,
    Byte1 assignee_privileges };
public struct {
    address registrant_address,
    String registrant_details,
    Byte1 registrant_status,
    Byte1 registrant_privileges,
    Integer registrant_reputation };
Constructor {
    main_registrar ← sender_address; }
PolicyControlModifiers {
    Is sender = main_registrar;
    Is sender = assignee_address;
    Is sender = registrant_address;
    Is assignee_privileges ≡ requested_task;
    Is registrant_privileges ≡ requested_task;
    Is sender_credit > transaction_value; }
```

```
ContractFunctions {
if sender = registrar then
    add_assignee();
    delete_assignee();
    update_assignee();
else
    retrun unauthorized;
end if
if sender = registrar || sender = assignee then
    add_registrant();
    delete_registrant();
    update_registrant();
else
    retrun unauthorized;
end if=0
```

Smart Contract ID Management

Algorithm 2 Contract ID_management

Require: *main_registrant address*

```
public address main_registrant;
public struct {
    address owner,
    String device,
    Byte20 attributes_hashedvalue
    Integer 1st_block,
    Integer last_block,
    Integer ID_revision,
    Byte1 identity_flags,
    Byte1 blocked_device };
public struct {
    Integer ID_revision,
    Integer previous_blockNo };
Constructor {
    main_registrant ← sender_address;
    owner ← sender_address; }
PolicyControlModifiers {
    Is sender = owner;
    Does ID exist;
    Is registrant_privileges ≡ requested_task;
    Is sender_credit > transaction_value; }
```

```
ContractFunctions {
if sender = owner then
    create_deviceIdentity();
    update_deviceIdentity();
    assign_device();
    withdraw_deviceIdentity();
else
    retrun unauthorized;
end if
if sender = registrar || sender = assignee then
    block_device;
    verifiy_deviceIdentity();
else
    retrun unauthorized;
end if
query_deviceIdentity_owner();
```

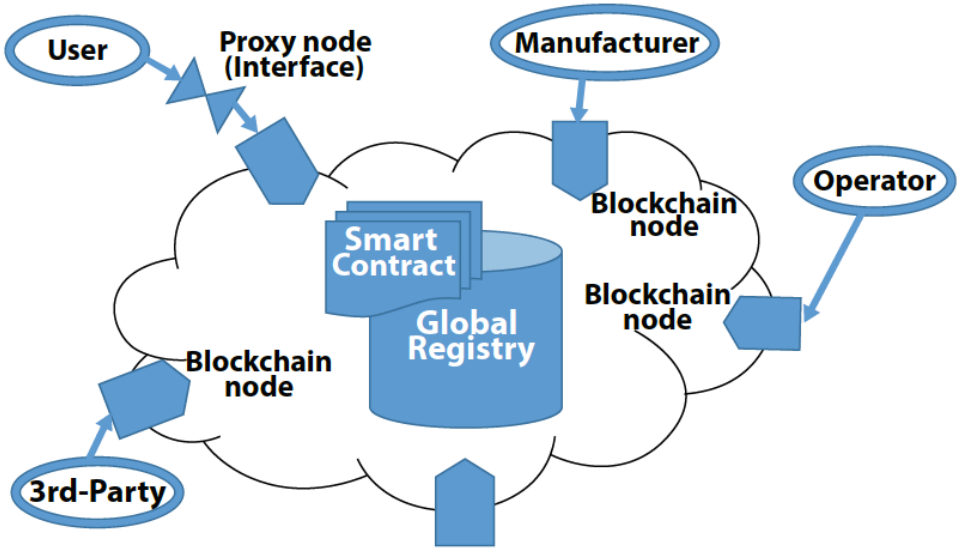
Smart Phone Counterfeiting

- The effect of counterfeiting on smart phone sales worldwide is estimated at 184 million units, valued at 45.3 billion EUR or 12.9 % of total sales.
- Additionally, this poses security, privacy, and even general safety concerns.
- Status-Quo is a single centralized database is maintained by the GSM Association and it is used to query on counterfeited devices.
  - Slow process to reflect reported loss, theft or counterfeiting report.
  - Access controlled by a single authority, dominated by big players.

”The Economic Impact of Intellectual Property Rights (IPR) Infringement in Smartphone Sector,” Rep. European Union Intellectual Property office, Feb. 2017

Features

- A distributed Blockchain-based ledger for registration, query, and verification of counterfeited phones.
- An open global registry
  - IMEI as the main attribute, in addition to the model and serial numbers.
- Interested parties, such as operators, distributors, IP protection agencies and consumers can query and verify a phone digital identity.



Conclusion

- A Blockchain-based digital identity and an identity management approach that ensures a global and unique device identity.
- Utilizing the underlying Blockchain functions and features, specifically cryptographic assets, immutability and provenance.
- A framework that defines the process required for identity creation and both identity validation and tracing.
- Providing the means to handle devices ownership and identity management throughout the device life cycle.