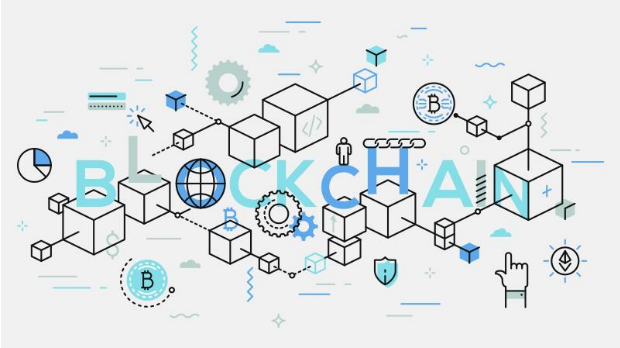
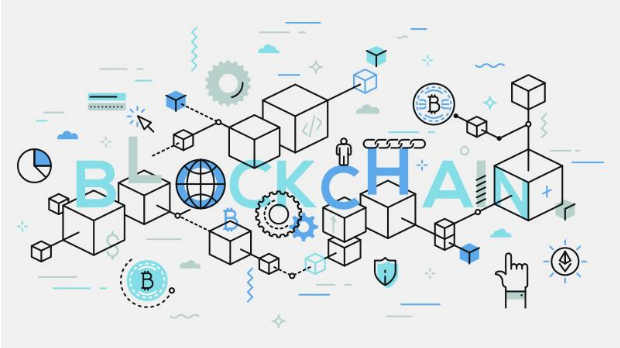
Using Blockchains for GDPR verification

Presented by: Masoud Barati

November 2019

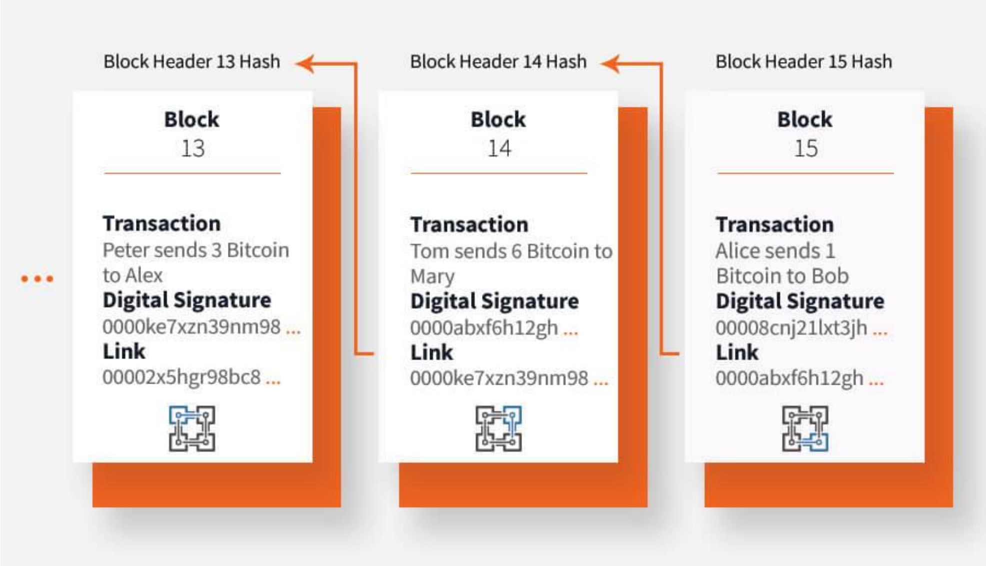


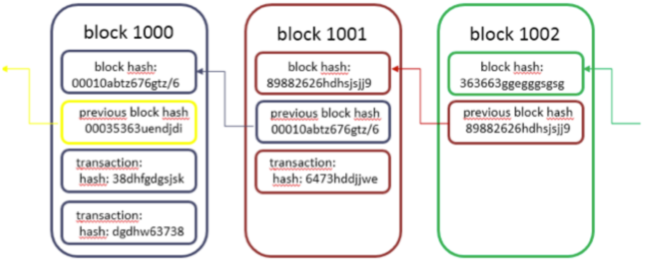
Blockchain



Blockchain concept

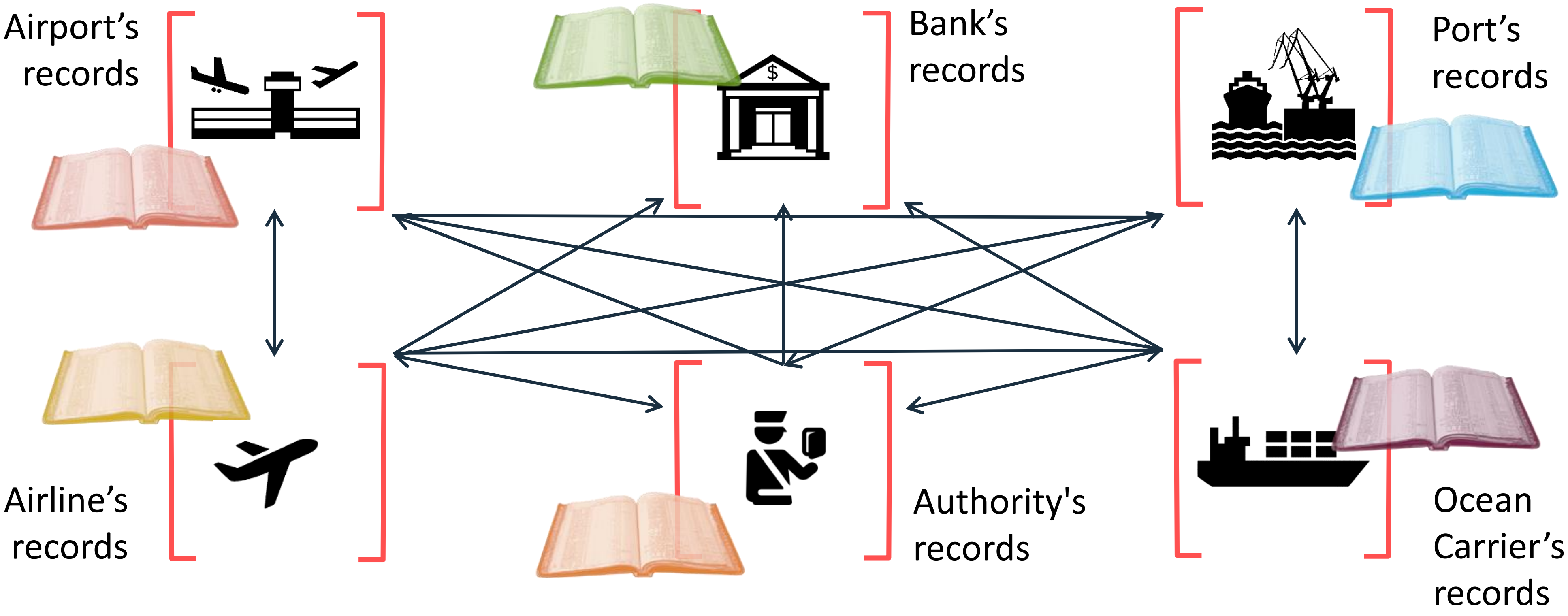
- Is a public ledger involving a set of blocks:
  - Blocks are created by miners (nodes)
  - Each block contains a number of transactions
  - Blocks are distributed across the network (Internet)-everyone has a copy
  - Blocks are immutable- No transaction can be deleted
  - Blocks are accessible to all
  - Transactions inside blocks are encrypted





Why Blockchain…complex records

Recording of events is becoming much more complex…



… Inefficient, expensive, vulnerable, lack of transparency

Why Blockchain…

- The Database needed
- There are multiple writers
- Writers are unknown
- Cannot rely on trusted third party

REDUCES COST
by eliminating manual processes (ex. reconciliation between multiple isolated ledgers, administrative processes, etc.)

INCREASED SPEED
of transaction and settlements through immediate distribution

INCREASED SECURITY
through use of cryptography

REDUCED FRAUD
by time-stamping entries and sharing a common, immutable ledger across the network

REDUCED RISK
of single points of failure & attack through distributed network nodes

Blockchain for business

Distributed **system of record** shared across business network

Business terms embedded in transaction database & executed with transactions

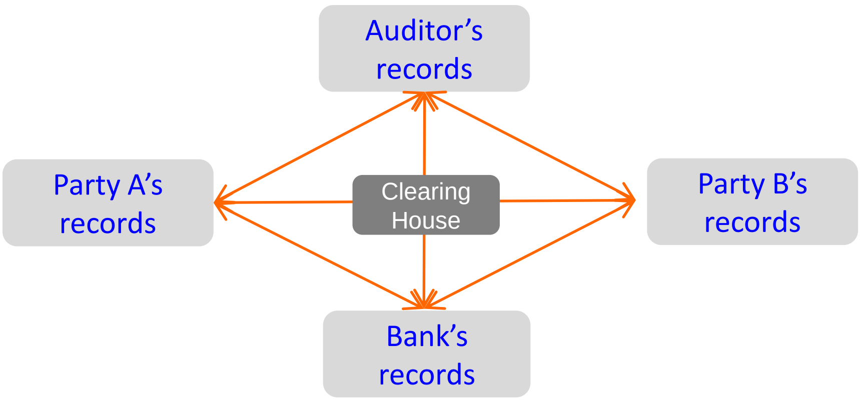
Ensuring appropriate visibility; transactions are secure and verifiable

All parties agree to network verified transaction

… Broader participation, lower cost, increased efficiency

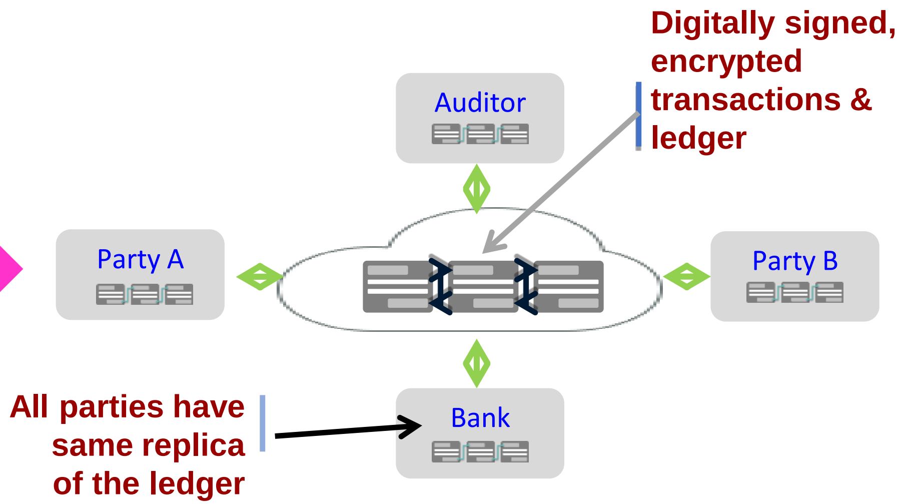
Blockchain changes business

Traditional Way



… Inefficient, expensive, vulnerable

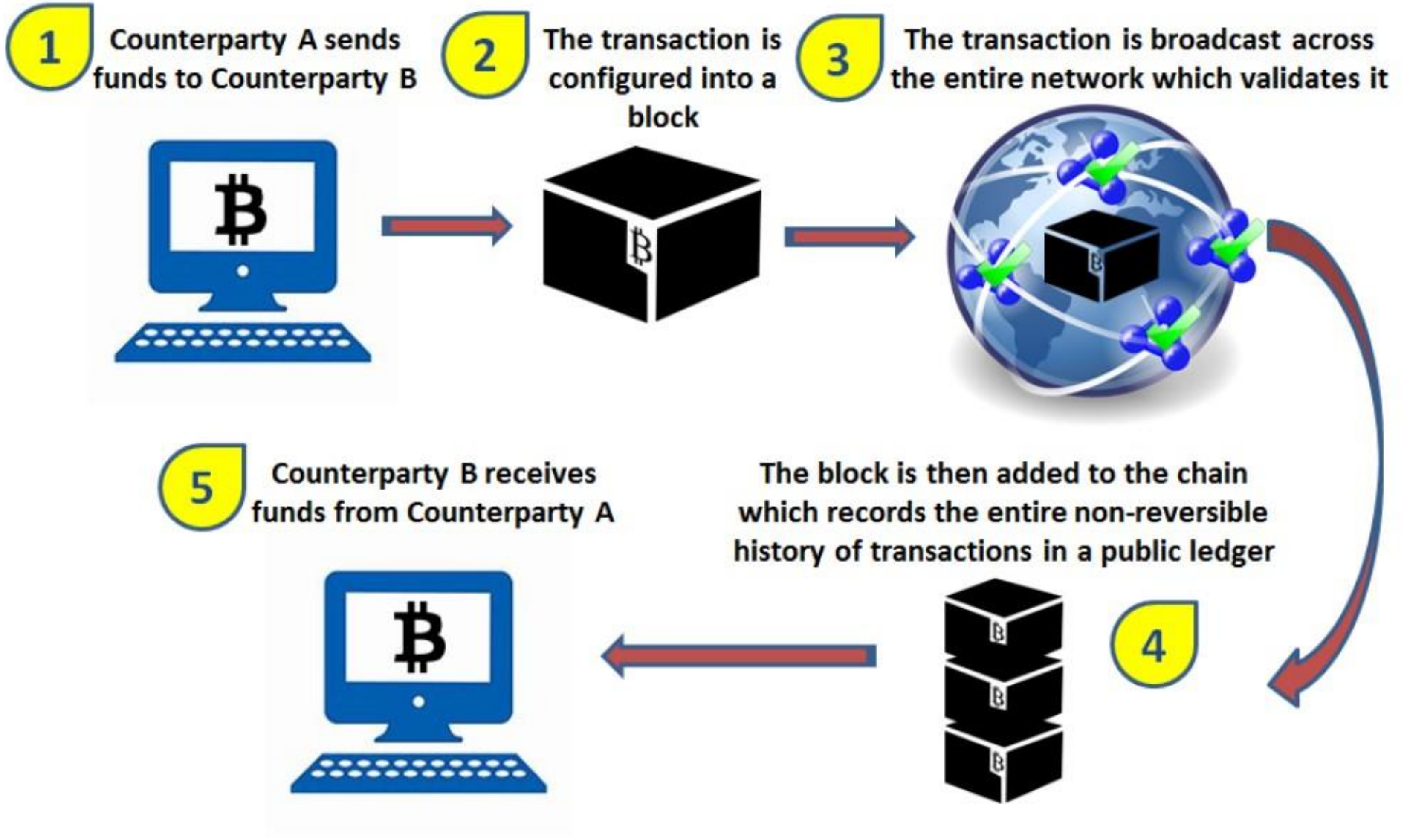
Blockchain Way



… Consensus, provenance, immutability

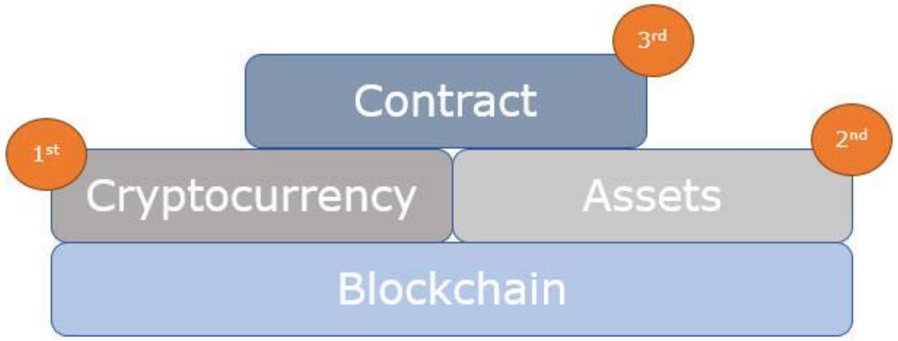
A Blockchain-based example

Money transfer between two parties

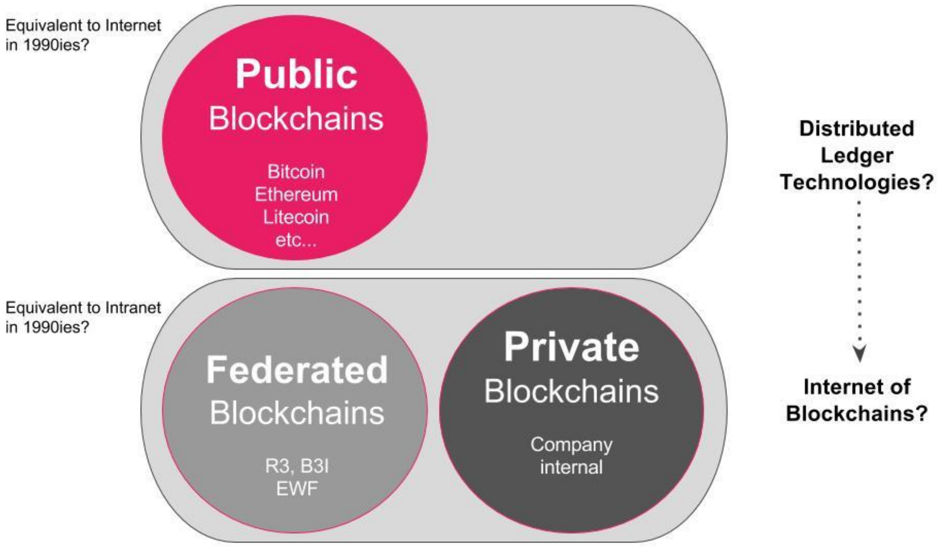


Generation and classification

- **Generations:**
  - First generation: bitcoins
  - Second generation: exchanges assets, goods and even votes
  - Third generation: smart contracts



- **Classes:**
  - Public--blocks are accessible to all and everyone can be miner
  - Federated--blocks are accessible for a group of authorized people in multiple organization with valid miners
  - Private--blocks are accessible only for authorized people registered in an organization and created by only a limited number of trusted miners



Miners and techniques

Miners:

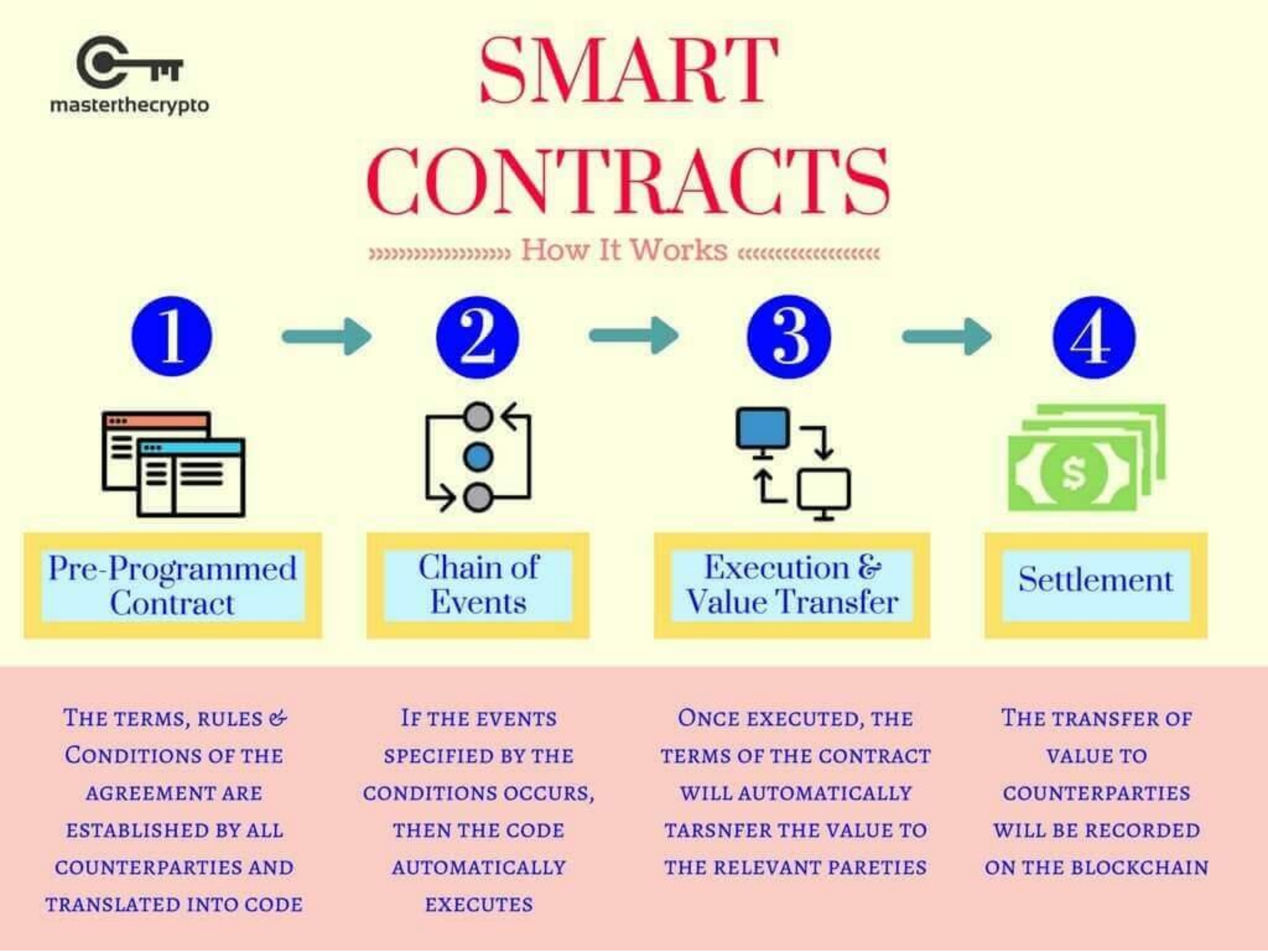
- are peer to peer nodes creating blocks and validate transactions.
- compete to solve a difficult mathematical problem based on a cryptographic hash algorithm.
- apply following techniques for mining blocks:
  - Proof of Work (PoW)
  - Proof of Stake (PoS)
  - Practical Byzantine Fault Tolerance (PBFT)
  - Proof of space (PoSpace)

  …

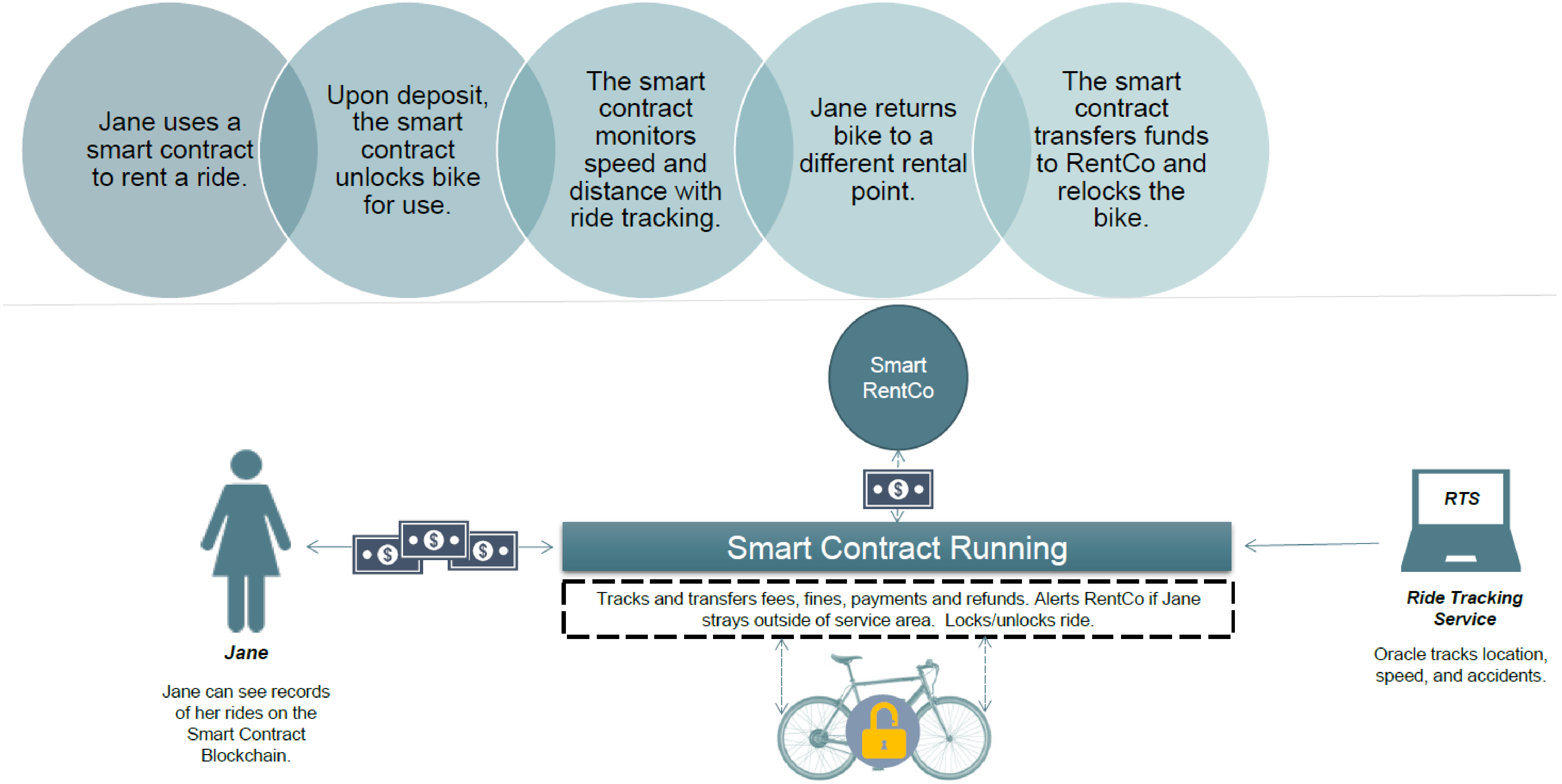
Smart contracts

- Is a programming codes in Solidity, Python,…
  - Translates conditions of contract as codes
  - Involves a set of functions
  - Store outputs of functions as events in Blockchain

```
contract MetaCoin {
  mapping (address => uint) balances;

  function MetaCoin() {
    balances[tx.origin] = 10000;
  }

  function sendCoin(address receiver, uint amount) returns(bool sufficient) {
    if (balances[msg.sender] < amount) return false;
    balances[msg.sender] -= amount;
    balances[receiver] += amount;
    return true;
  }

  function getBalance(address addr) returns(uint) {
    return balances[addr];
  }
}
```

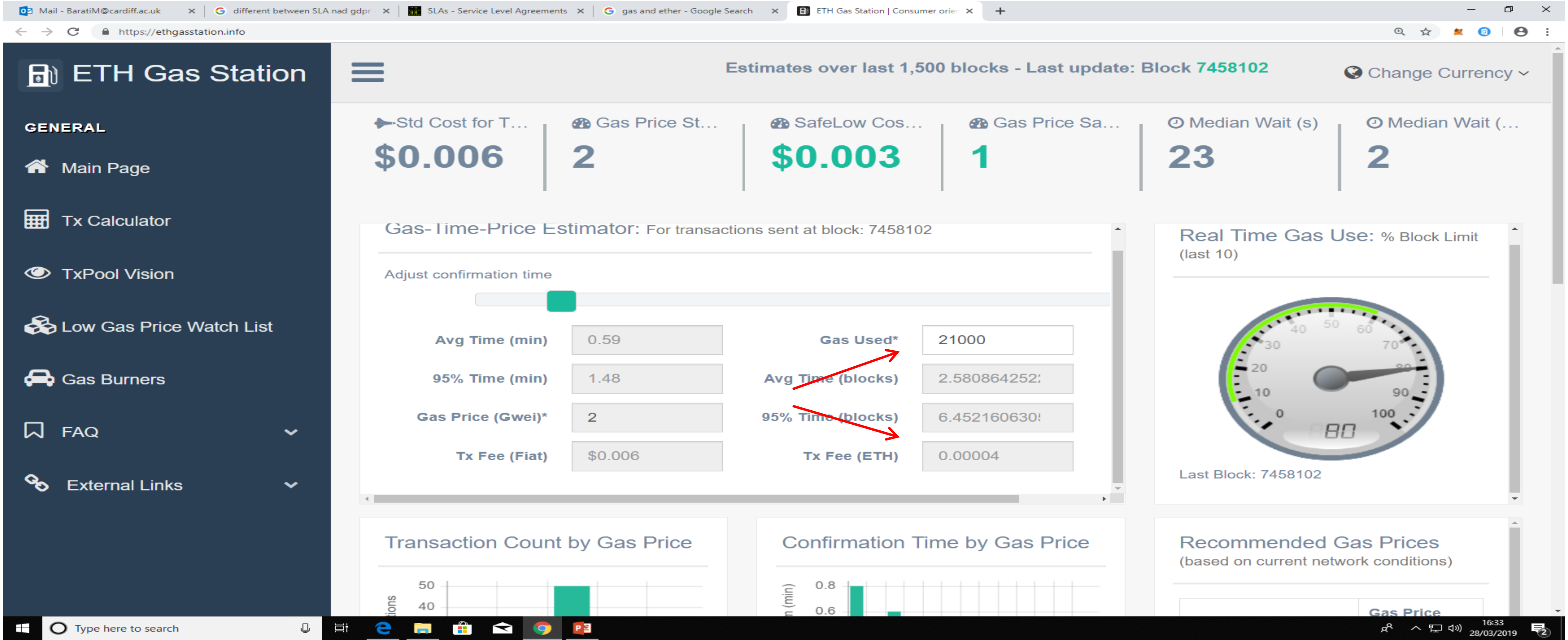


An example of smart contracts

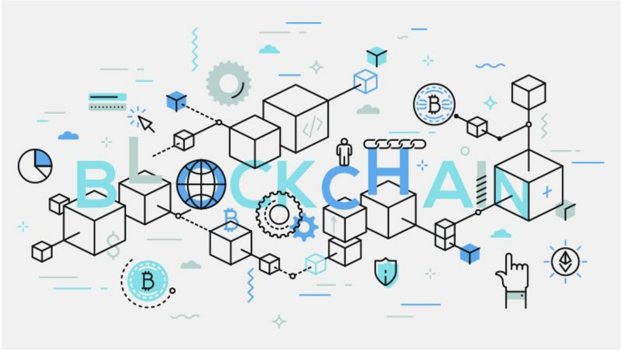


Key notions: gas & ether

- Gas: is the internal pricing for running a transaction
- Ether: is a fuel given to miner to run smart contract



Verifying GDPR via Blockchain



Integration of GDPR and Blockchain

- How to track the audit trail of data controllers/processors?
  - Accountability through Blockchain
- How to implement smart contracts for verifying GDPR rules?
- What GDPR rules are checked through smart contracts?
- How to design an architecture for interacting controller/processor and data subjects with smart contracts?
- Who will check the Blockchain and notify any GDPR violation?

Implementation of intended GDPR rules

Read

- **L1**: Does your service deal with sensitive personal data?
- **L2**: Does your service support encryption or authentication access for the customer data?

Write

- **L1**: Does your service enable customers delete their data in the original used service?
- **L2**: How long will the personal data be stored?
- **L3**: How long is it necessary for processing personal data through your service?

Profiling

- **L1**: Does your service avoid automated profiling on the personal data of customer who is under 18?
- **L2**: Does your service avoid automated profiling on sensitive personal data?

Transfer

- **L1**: Does your service give the choice of EU-based migration of personal data?
- **L2**: Has your underlying connected provider been certified for their Binding Corporate Rules (BCR) clauses by a EU DPA?

Algorithm 2 The function of read operation

Input: add_a, D_r, $encrypt$
Output: add_a, D_r, $compliance$

function READ
  $compliance$ = `true`;
  if $encrypt$ == `false` **then**
    $compliance$ = `false`;
  return$(add_a, D_r, compliance)$;

Algorithm 3 The function of write operation

Input: add_a, D_w, $erase$, $\mathcal{T}_t$, $\mathcal{T}_s$
Output: add_a, D_w, $compliance$

function WRITE
  $compliance$ = `true`;
  if $erase$ == `false` or $\mathcal{T}_t < \mathcal{T}_s$ **then**
    $compliance$ = `false`;
  return$(add_a, D_w, compliance)$;

Algorithm 4 The function of profiling operation

Input: add_a, D_p, $isadult$, $sensitive$
Output: add_a, D_p, $compliance$

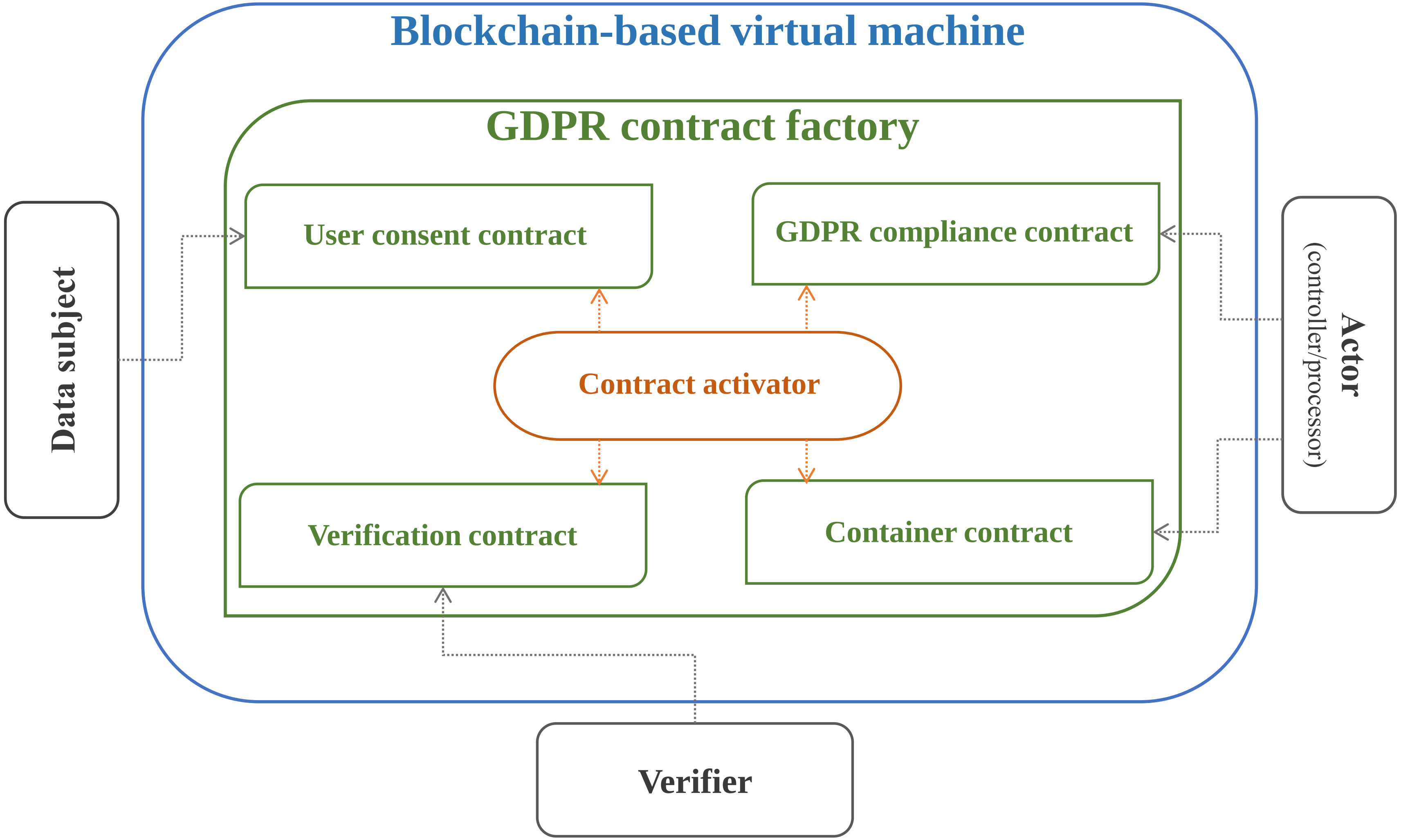
function PROFILING
  $compliance$ = `true`;
  if $isadult$ == `false` or $sensitive$ == `true` **then**
    $compliance$ = `false`;
  return$(add_a, D_p, compliance)$;

Algorithm 5 The function of transfer operation

Input: add_a, D_t, loc
Output: add_a, D_t, $compliance$

function TRANSFER
  $compliance$ = `true`;
  if $loc \notin EU$ **then**
    if $loc \notin BCR$ **then**
      $compliance$ = `false`;
  return$(add_a, D_t, compliance)$;

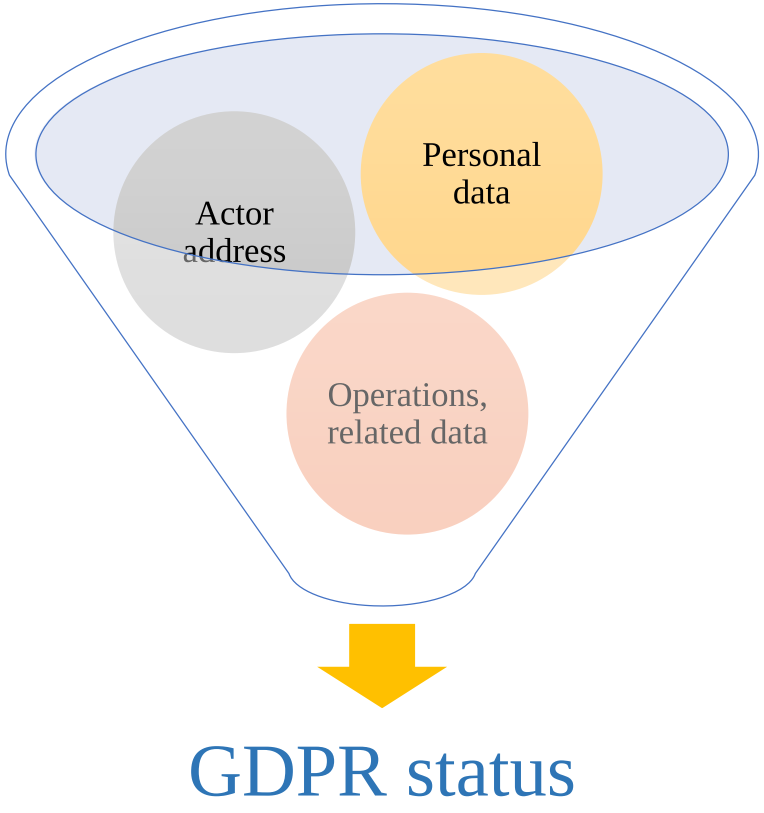
Architecture



GDPR compliance contract

- Gets following information from data controller/processor (actor):
  - The address of actor
  - The personal data that are demanded by actor
  - The operation that will be executed on personal data
  - Some data related to the GDPR legal questions

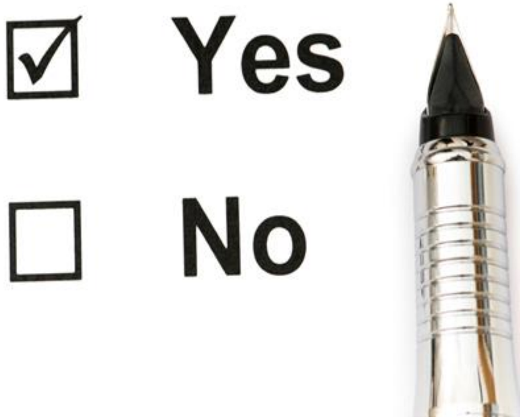
- Output:
  - Status of GDPR compliance



User consent contract

- It has two functions:
  - One for retrieving the blocks created by GDPR compliance contract
    - What is next operation
    - GDPR status of operation
    - What personal data must be provided

  - One for receiving the consent or negate of data subject
    - Record vote (consent/negate) in Blockchain for the aim of future verification



Container contract

- It records following information in Blockchain:
  - Actor address
  - Processed/ accessed personal data
  - Executed operations (e.g., transfer, store, etc.)

Such records are utilized for the aim of verification

- It gives data subjects the right to access:
  - Where data is processing
  - History of data movement

Verification contract

It checks:

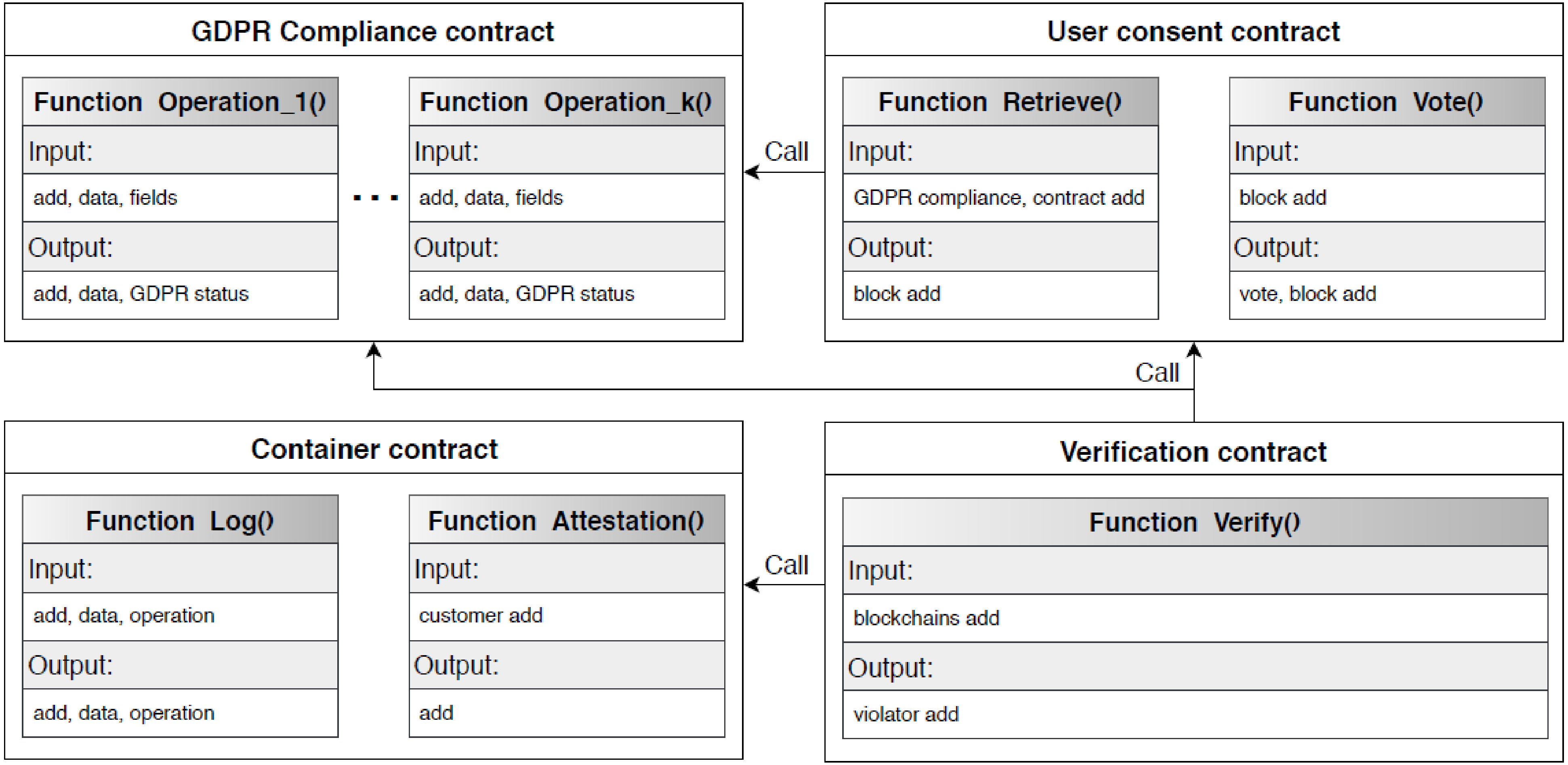
- whether the **addresses of actors** recorded by container contract conform to those recorded via GDPR compliance contract or not;

- whether the **operations** of each actor recorded by container contract conform to those recorded via GDPR compliance contract or not;

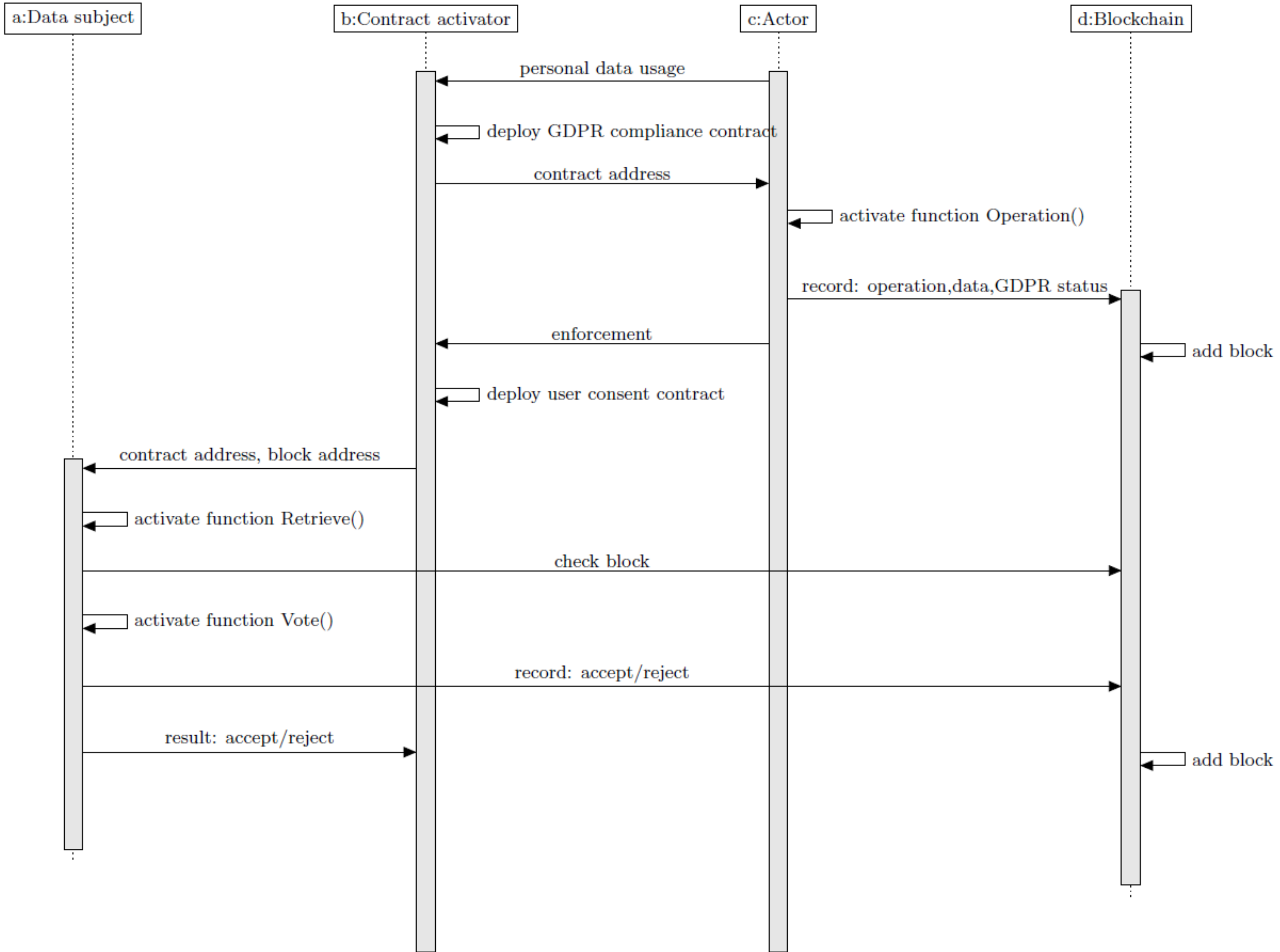
- whether the **personal data** processed by each operation and recorded via container contract conform to those claimed by GDPR compliance contract or not;

- whether the operations of each actor recorded by container contract were **already confirmed** by data subject or not;

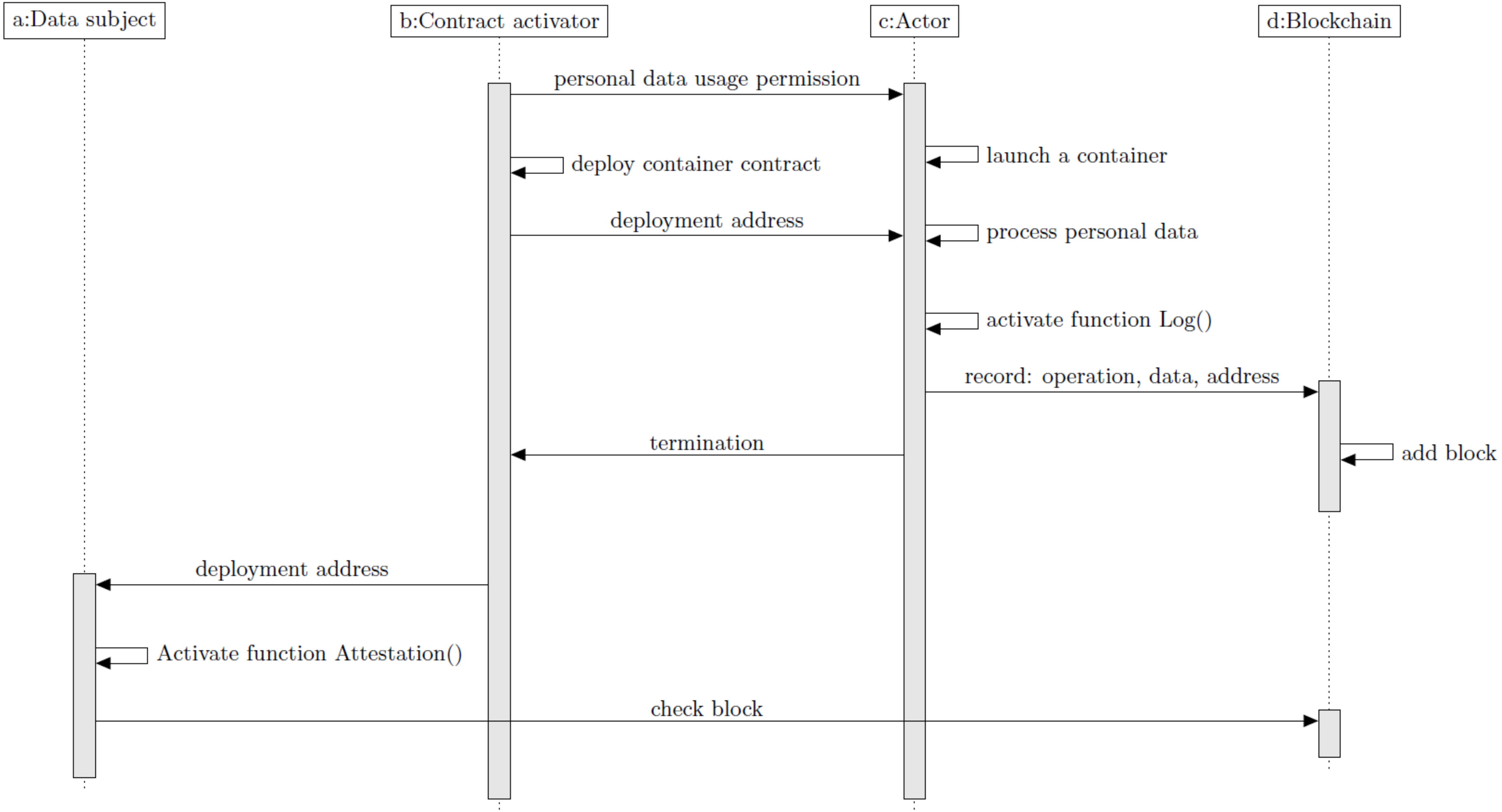
Abstract model of smart contracts



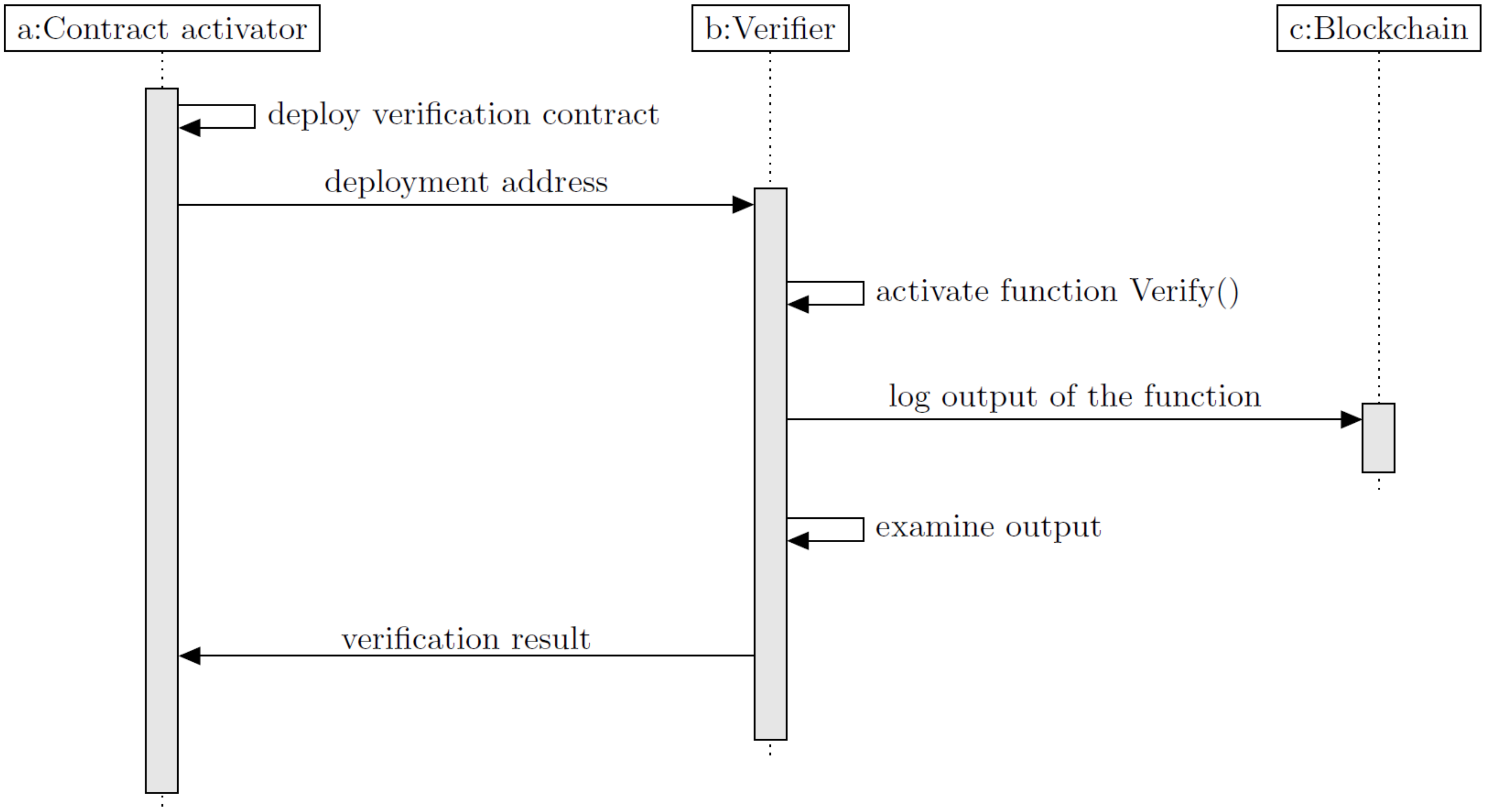
A protocol for receiving user consent



A protocol for submitting events to Blockchain



A protocol for verifying blocks



Verification – violation detection

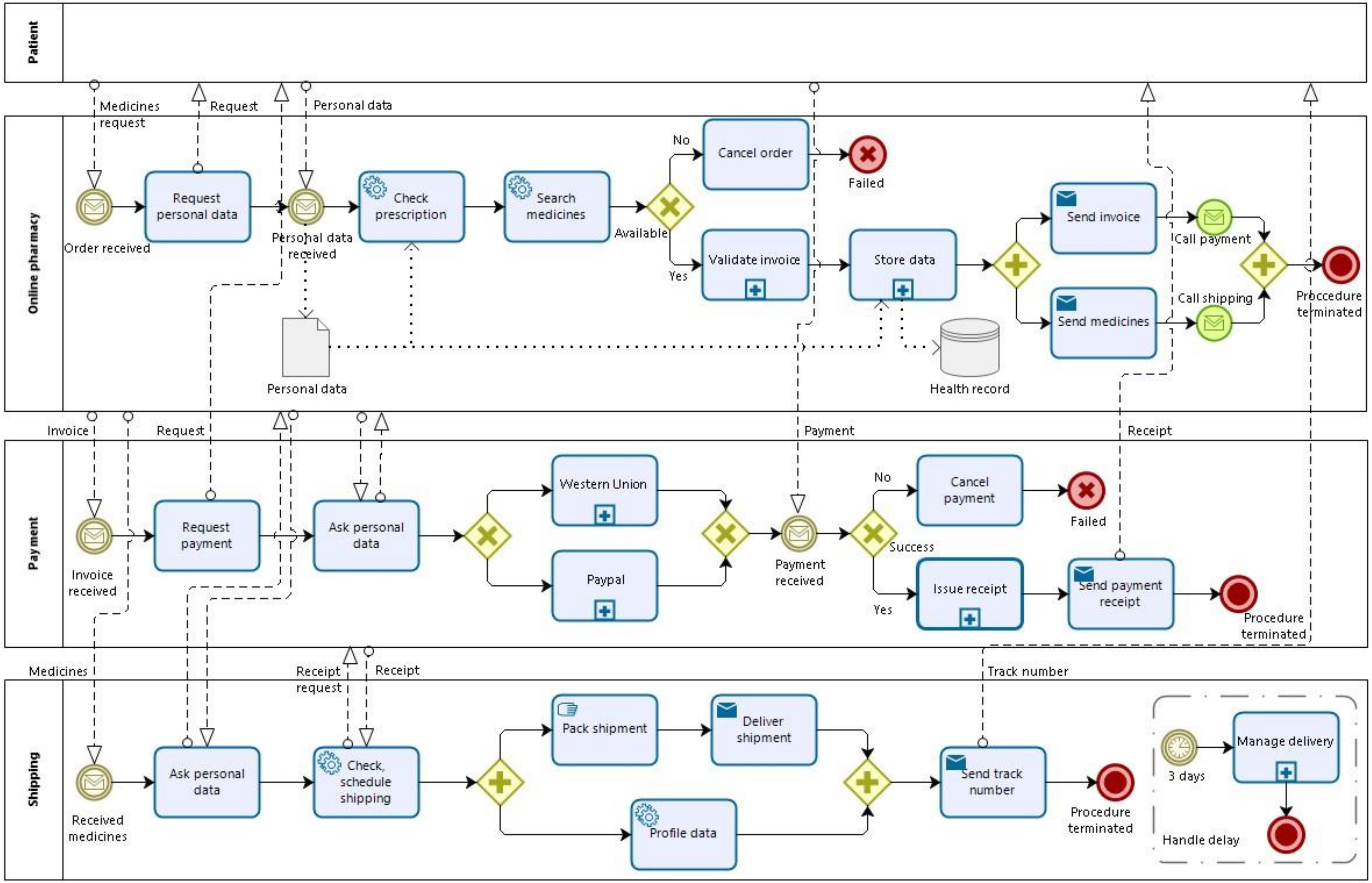
- The actor address processing personal data
- The operations executed on personal data by actor
- The personal data processed by actor

Algorithm 1 The verification of actors

Let $\mathcal{V}$ be a set containing violators' addresses
Input: customer address
Output: $\mathcal{V}$

function VERIFY
    $\mathcal{V} \leftarrow \emptyset$;
    if $A_e \not\subseteq A_c$ **then**
        $\mathcal{V} \leftarrow \mathcal{V} \cup A_e \backslash A_c$;
    for all $a \in A_c$ **do**
        if $Op_a^e \not\subseteq Op_a^c$ **then**
            $\mathcal{V} \leftarrow \mathcal{V} \cup \{a\}$;
        if $\mathcal{D}_{op}^a \not\subseteq D_{op}^a$ **then**
            $\mathcal{V} \leftarrow \mathcal{V} \cup \{a\}$;
    return $\mathcal{V}$;

A scenario


Patient
Online pharmacy
Payment
Shipping
Medicines request
Request
Personal data
Order received
Request personal data
Personal data received
Check prescription
Search medicines
Available
No
Yes
Cancel order
Failed
Validate invoice
Store data
Send invoice
Send medicines
Call payment
Call shipping
Proccedure terminated
Personal data
Health record
Invoice
Request
Payment
Receipt
Invoice received
Request payment
Ask personal data
Western Union
Paypal
Payment received
No
Success
Yes
Cancel payment
Failed
Issue receipt
Send payment receipt
Procedure terminated
Medicines
Receipt request
Receipt
Track number
Received medicines
Ask personal data
Check, schedule shipping
Pack shipment
Deliver shipment
Profile data
Send track number
Procedure terminated
3 days
Manage delivery
Handle delay

Required personal data

- **Pharmacy service provider** asks some patient data: **name, address details, age, electronic version of prescription, and bank account details**. It provides the **payment service provider** some personal data, including name and bank account details. It also **sends** the name and address details of patient to the **shipping service provider** to deliver medicines. The provider **maintains** the medical information of patients to provide a comprehensive understanding of patients' records for the healthcare professionals.

- **Payment service provider** accesses the personal data, e.g., **bank account details**, provided by the pharmacy service provider to organize the payment process and transfer money.

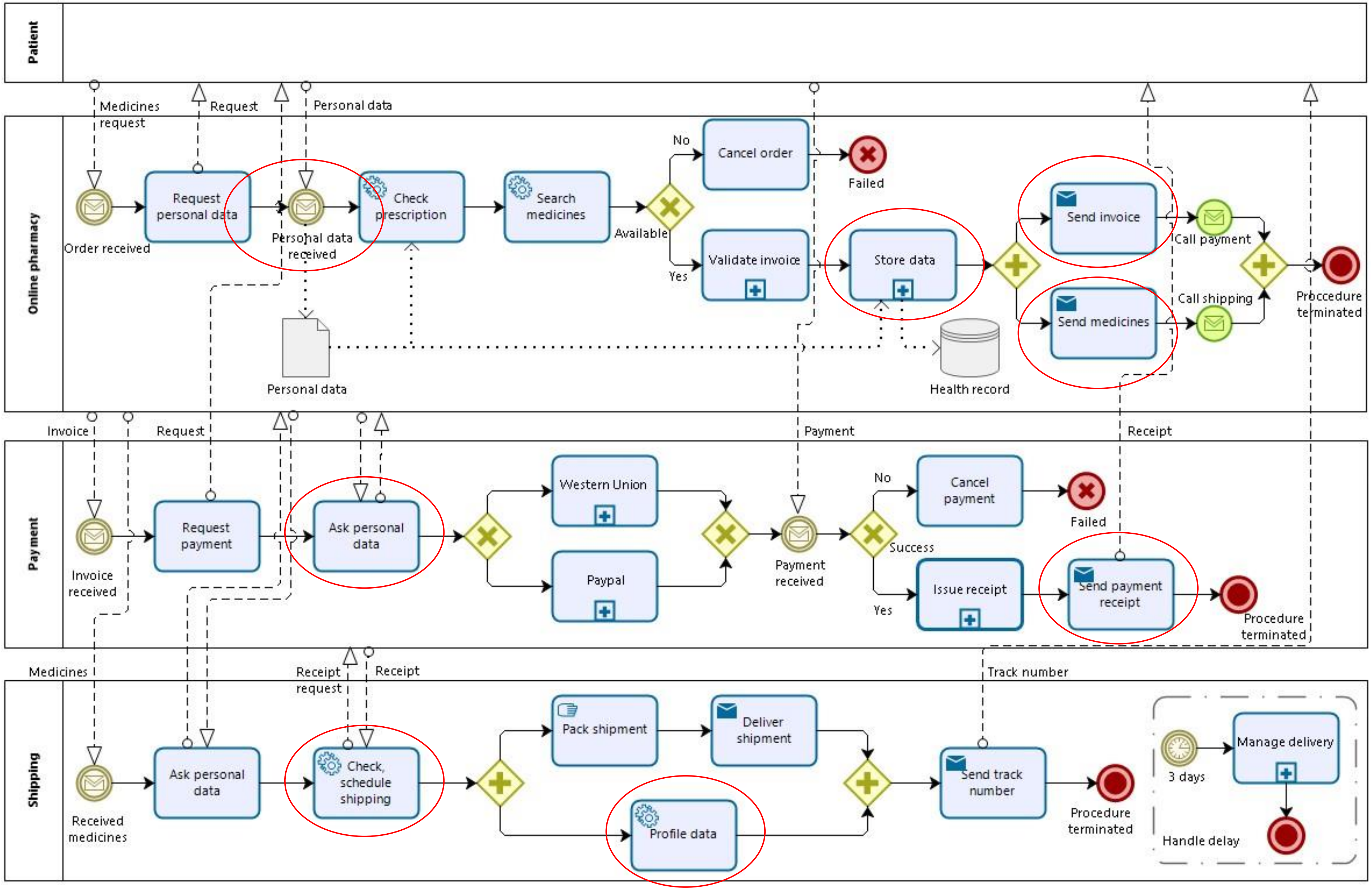
- **Shipping service provider** receives the personal data provided by the pharmacy service provider to manage the shipping of medicines. It runs a **profiling** operation on the **destination addresses** of its customers to obtain and publish some statistics.

GDPR roles

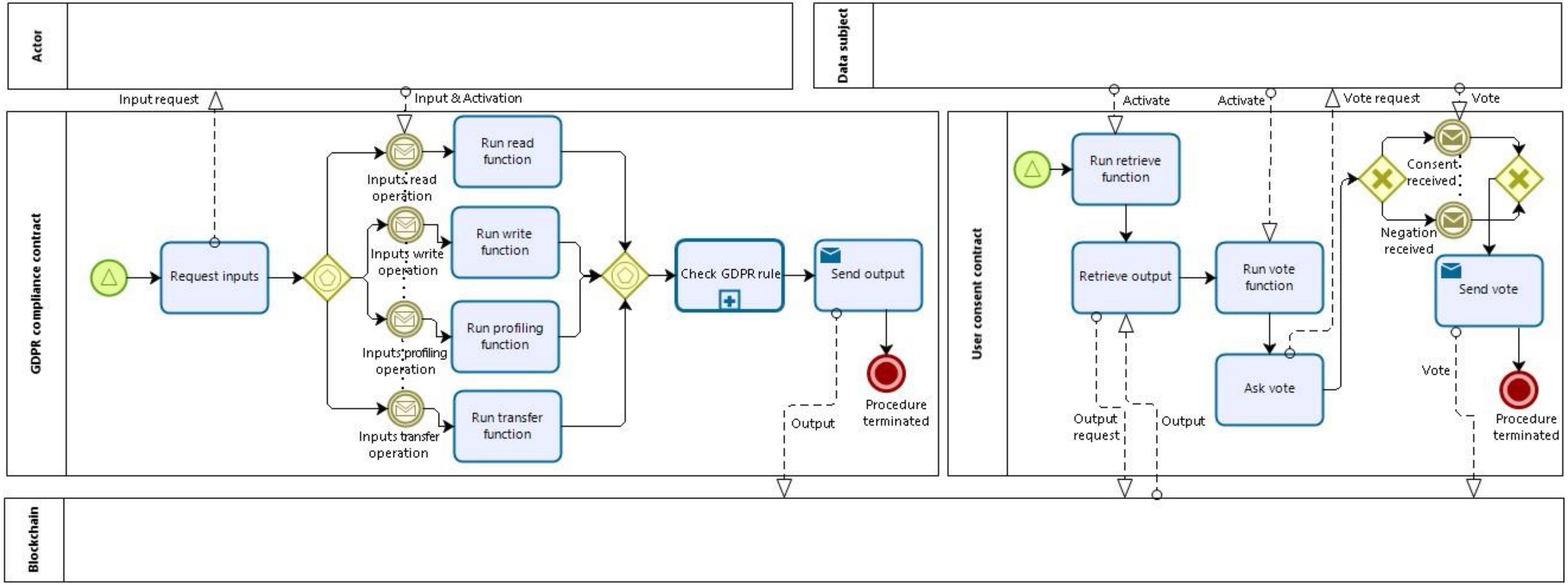
Controller, Processor

Controller, Processor

Processor

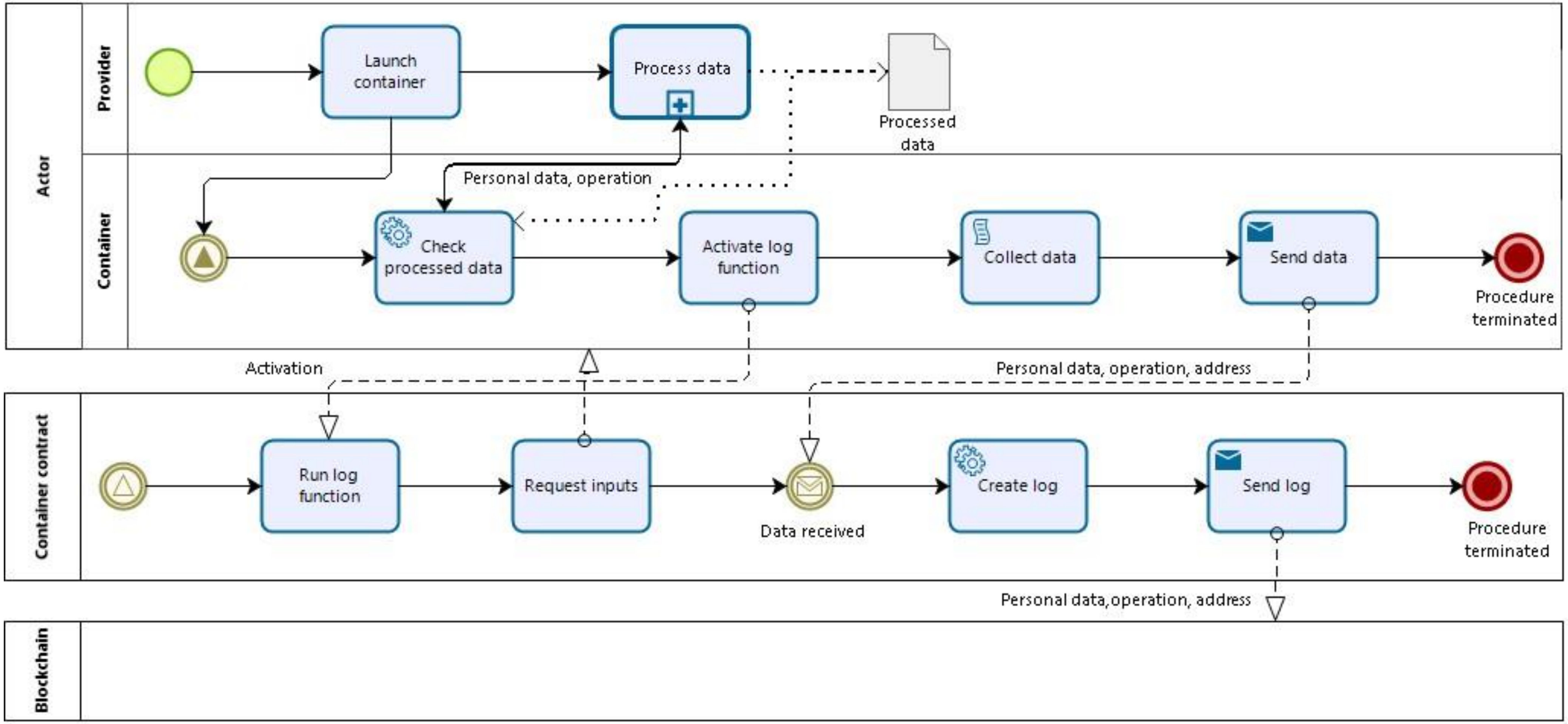


Initialization phase - data subjects & actors



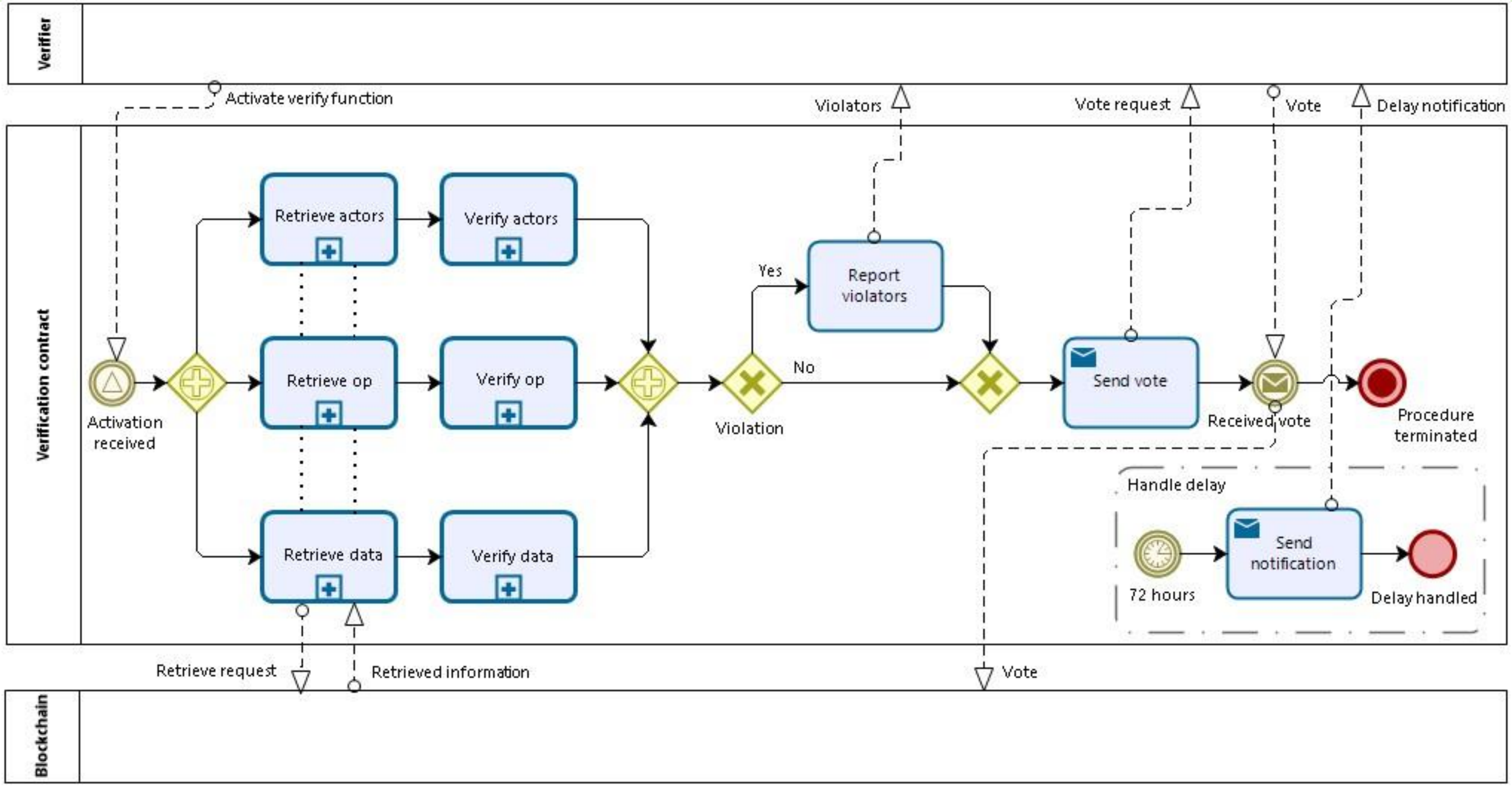
GDPR: User consent, evidence of consent, determining purposes of data processing, right to be informed

Submission phase



GDPR: Accountability, right to access

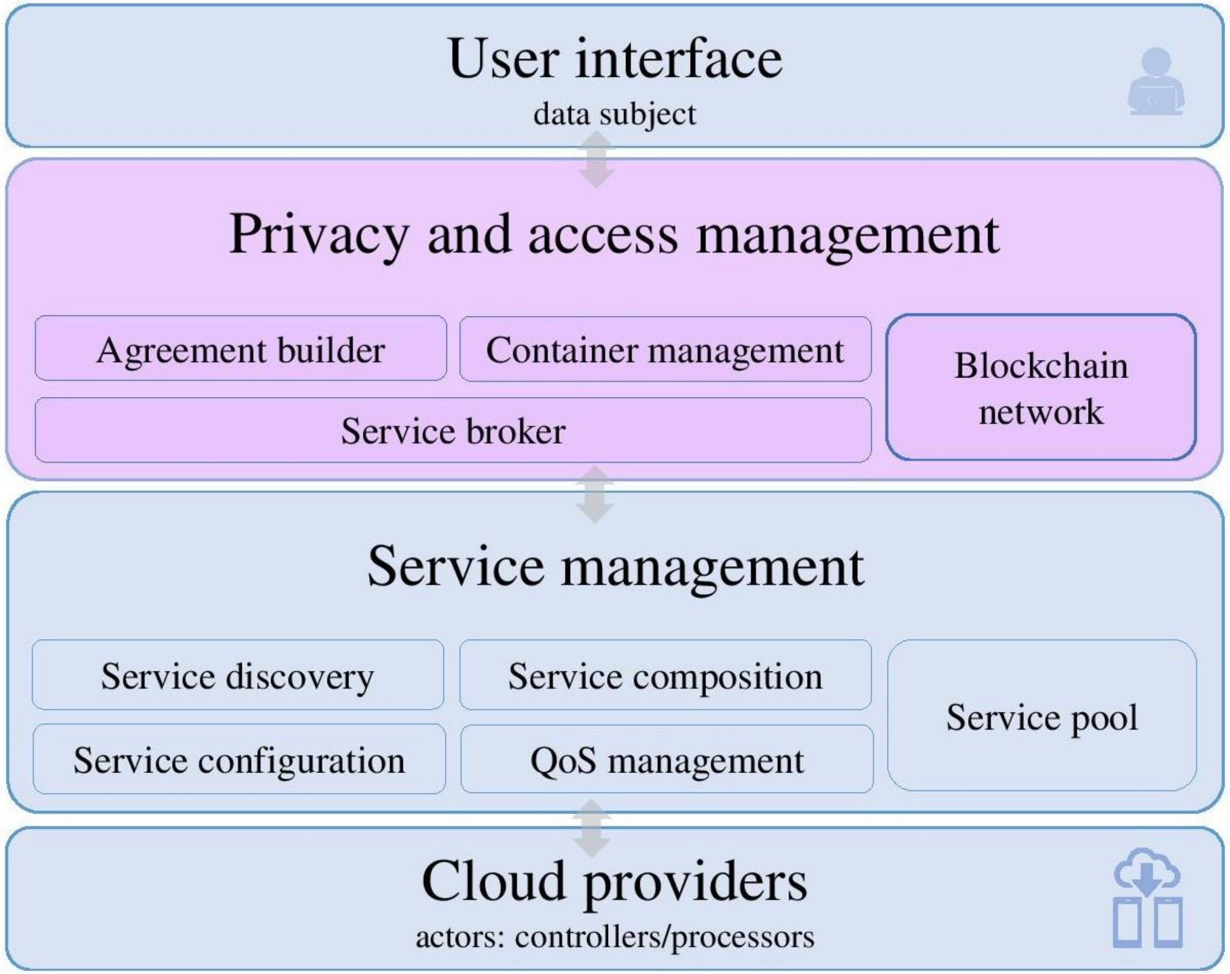
Verification phase



GDPR: Breach notification

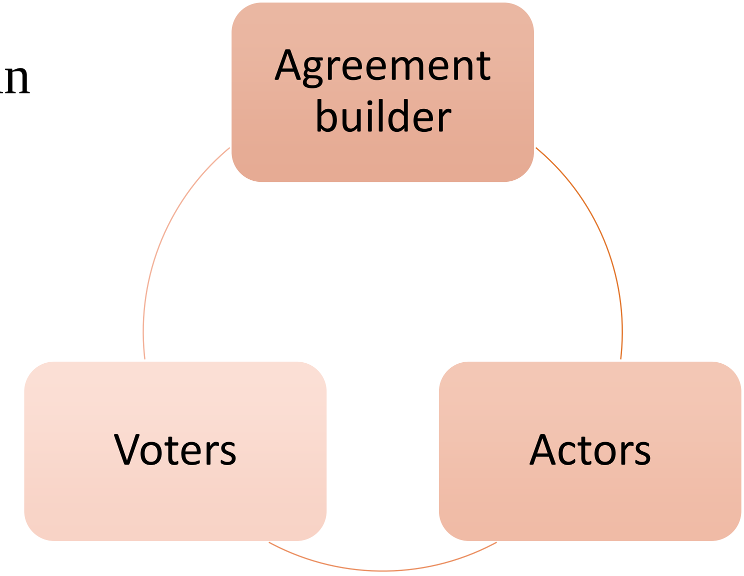
Contributions in Cloud and IoT

A privacy-aware cloud architecture



The idea behind privacy-aware cloud architecture

- **Agreement builder** is a third-party (broker) that connects to blockchain with following objectives:
  - Establish the negotiation between user and actors for reaching an agreement
  - Hold the smart contracts enabling the verification of actors
  - Orchestrate actors and voters for accessing or running the smart contracts



- **Actors** are providers with the roles of data controllers or processors

- **Voters** are a set of third-parties that connect to blockchain to report any violation

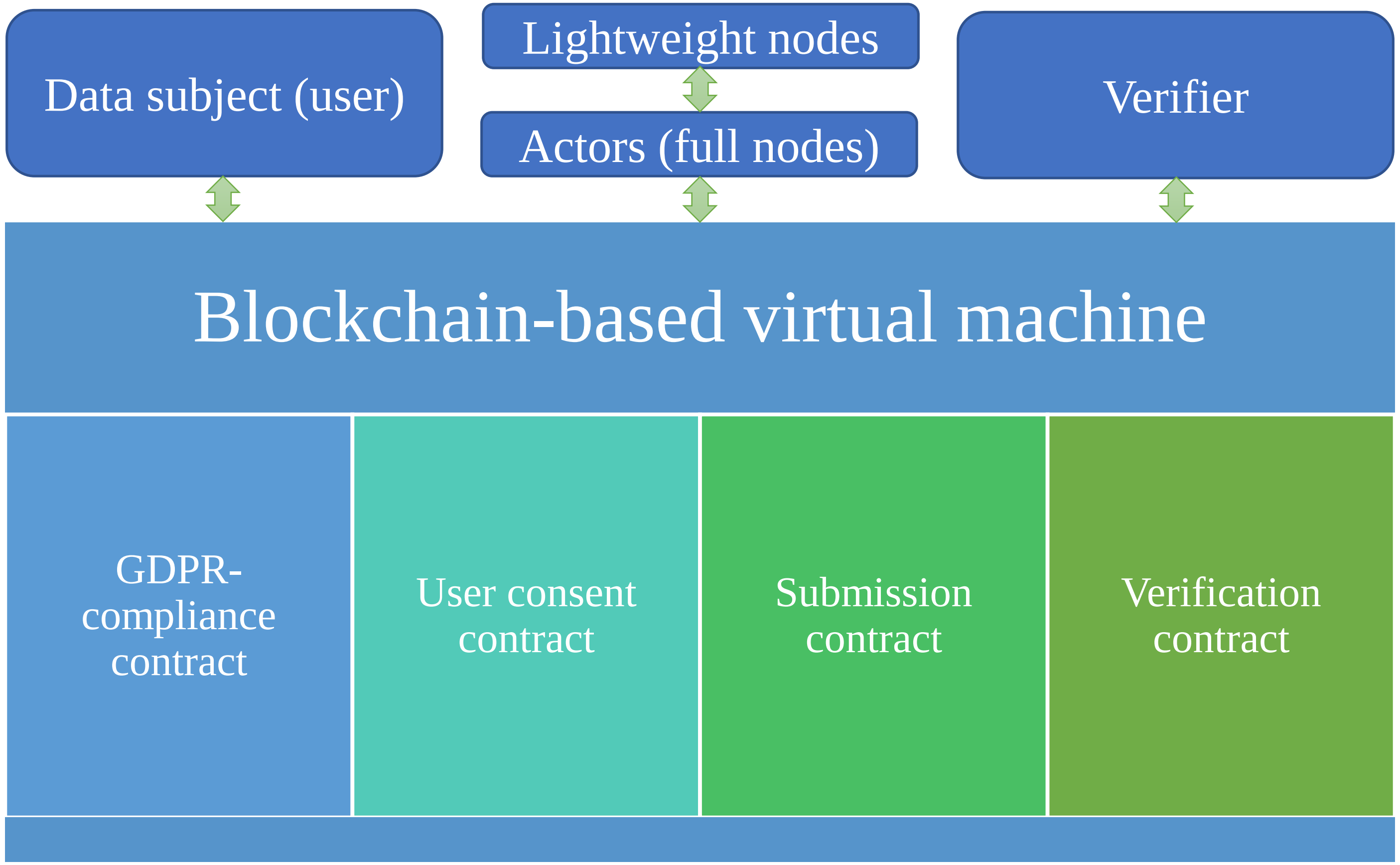
Degree of GDPR compliance

- **Fully-compliance:** the verification of operation must inevitably be verified under GDPR rules ($Deg(\alpha_i) = 1$), α_i is an operation

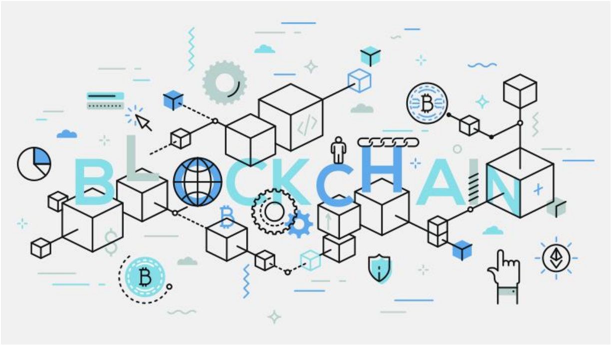
- **Partially compliance:** the verification has a lower level of importance for data subject ($0 < Deg(\alpha_i) < 1$)

- **Non-compliance:** the verification is never a concern for data subject ($Deg(\alpha_i) = 0$)

A blockchain-based architecture in IoT



Thank you very much for your attention



Who are processors, controllers?
What are purpose of data processing?
What are processing operations?
Personal data and level of sensitivity?