
Telsy


# Decentralised and secure analytics system

Andrea Di Nenno

CifrisChain 2018 - 17 Dicembre 2018 - Roma

# Decentralised

## Blockchain

Temper-proof, public, replicated ledger

Non repudiation of each writing operation

Connect mistrusting parties without intermediaries

## Smart Contract

General purpose computer program that runs on a blockchain

Self-enforces the contract logic built into the code when specified conditions are met

Comes up with a regular wallet and a storage space

# Secure

## Multi-party Computation

Candidate technology for
“Computation on
Encrypted Data”

Input Privacy
Output Integrity
Robustness
No Single Point of Trust

It allows to compute a function
between mistrusting parties
without a trusted third party

Obfuscates the inputs
through an additive
secret sharing scheme

# Complementary technologies

**Both technologies address problems where mutually mistrusting parties are involved, without a trusted third party**

## Blockchain & Smart Contracts

Create, regulate and enforce ad-hoc business logics and economic bindings among parties through an incontestable and shared ledger

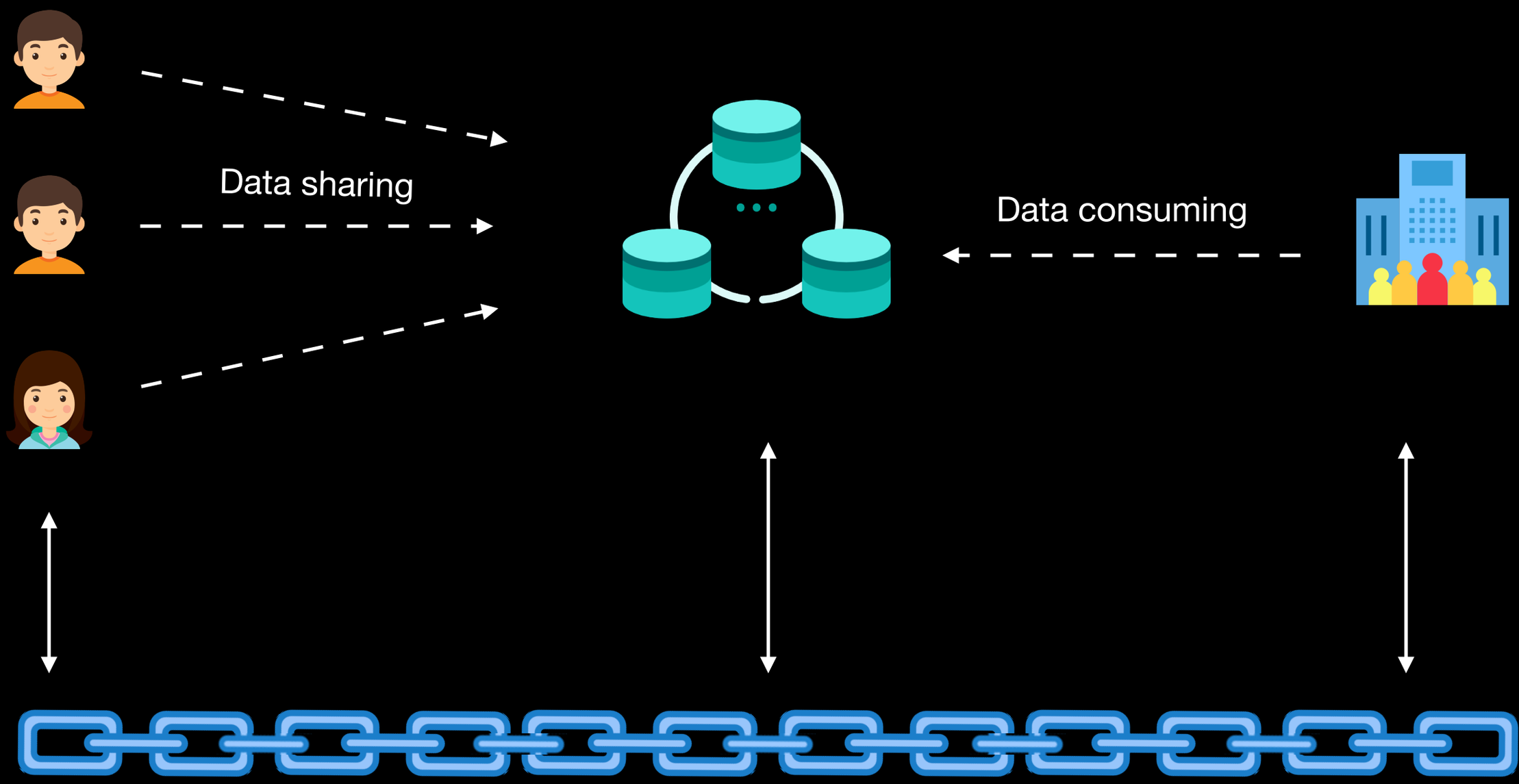
## MPC

Lets parties perform computations over their sensitive data maintaining them private

# Use Case

Sharing private medical data for research

**Data Producers** **MPC system** **Data Consumer**



# Use Case

Sharing private medical data for research

| Actor | Action | Benefit |
| --- | --- | --- |
| **Data Producer** (physical person) | Submits his medical private data in secret shared form | Gets rewarded every time his data is used and the privacy is guaranteed |
| **Data Consumer** (hospital or research) | Pays for data analytics calculations over private data | Access private medical data otherwise unavailable |
| **MPC System** (independent entities) | Runs multi-party computations | Gets rewarded for every correct computation or penalised otherwise |
| **Blockchain** | Manages authorisations<br>Logs what happens<br>Implements the business logic | |

# Data Consuming Protocol

**Data Consumer**

**Blockchain & Smart Contract**

**MPC servers**

DC request, $ deposit

dcID

Yes

Is he a data consumer?

dcID

Is this ID valid?

dcID

Yes

Have all servers accepted?

req accepted, $ deposit

Yes

Multi-party computation

# Data Consuming Protocol

**Data Consumer**

**Blockchain & Smart Contract**

**MPC servers**

Computation output

output hash

Have all servers sent the hash?

Yes

Are all hashes equal?

Yes

No

**Rewarding procedure**

**Penalisation procedure**

# Finalisation

Enforced by Smart Contract after each computation

## Rewarding procedure

**In case the computation delivered a correct output to the data consumer**

Data producers are rewarded with the data consumer's deposit

The MPC system gets his deposit back and is rewarded with the data consumer's deposit

## Penalisation procedure

**In case the computation aborted due to different outputs or timeout**

Data consumer gets his deposit back. The computational costs paid before are refunded with the MPC's deposit

The MPC system loses his deposit and isn't rewarded

# To Do

## Automatic cheater detection

Implement in a Smart Contract a logic to detect which MPC server cheated during the computation

## Scalability analysis

Number of servers
Function to compute
Data input size

## Reputation system

MPC servers may have a score indicating how they behaved on past computations

This score will influence the probability of a server to be selected for the next computation

# Used technologies

## SPDZ

Nigel Smart, Ivan Damgård

Open source base architecture written in C++

Multi-party computation programs written on top of it in Python

Communication with blockchain via Javascript Web3.js

## Ethereum & Solidity

Vitalik Buterin

Ethereum is the first blockchain implementing smart contracts

The EVM is Turing-complete

Solidity is an high-level, contract-driven programming language specifically designed for Ethereum


# Decentralised and secure analytics system

Andrea Di Nenno

CifrisChain 2018 - 17 Dicembre 2018 - Roma