Security infrastructure for distributed computing systems on the basis of blockchain technology*

A. Kryukov#, A. Demichev

Skobektsyn Institute of Nuclear Physics,
Lomonosov Moscow State University

* The work was supported by the Ministry of Science and Education of the Russian Federation, the Agreement No. 14.604.21.0146 (RFMEFI60414X0146).

E-mail: kryukov@theory.sinp.msu.ru

Outline

- Introduction
- Security in Distributed Computing System(DCS)
- Blockchain technology
  - Hashes, Merkle tree
  - Smart contract
  - Ethereum
- Blockchain in security infrastructure of DCS
- Conclusion

- I will not consider the cryptographic algorithms and protection communication channel.

Introduction

- Distributed computing systems (DCSs) are widely used by the researchers to solve different computational problems in various fields of natural science. DCS's are especially popular in the computer simulation in physics.
- One of the most significant examples of DCS is the EGI, including the WLCG, which is used for processing and simulation of experimental data from the LHC. The brilliant result of the LHC experiments is the discovery of Higgs boson, which could not be reached without the WLCG.

Security in Distributed Computing System (1/3)

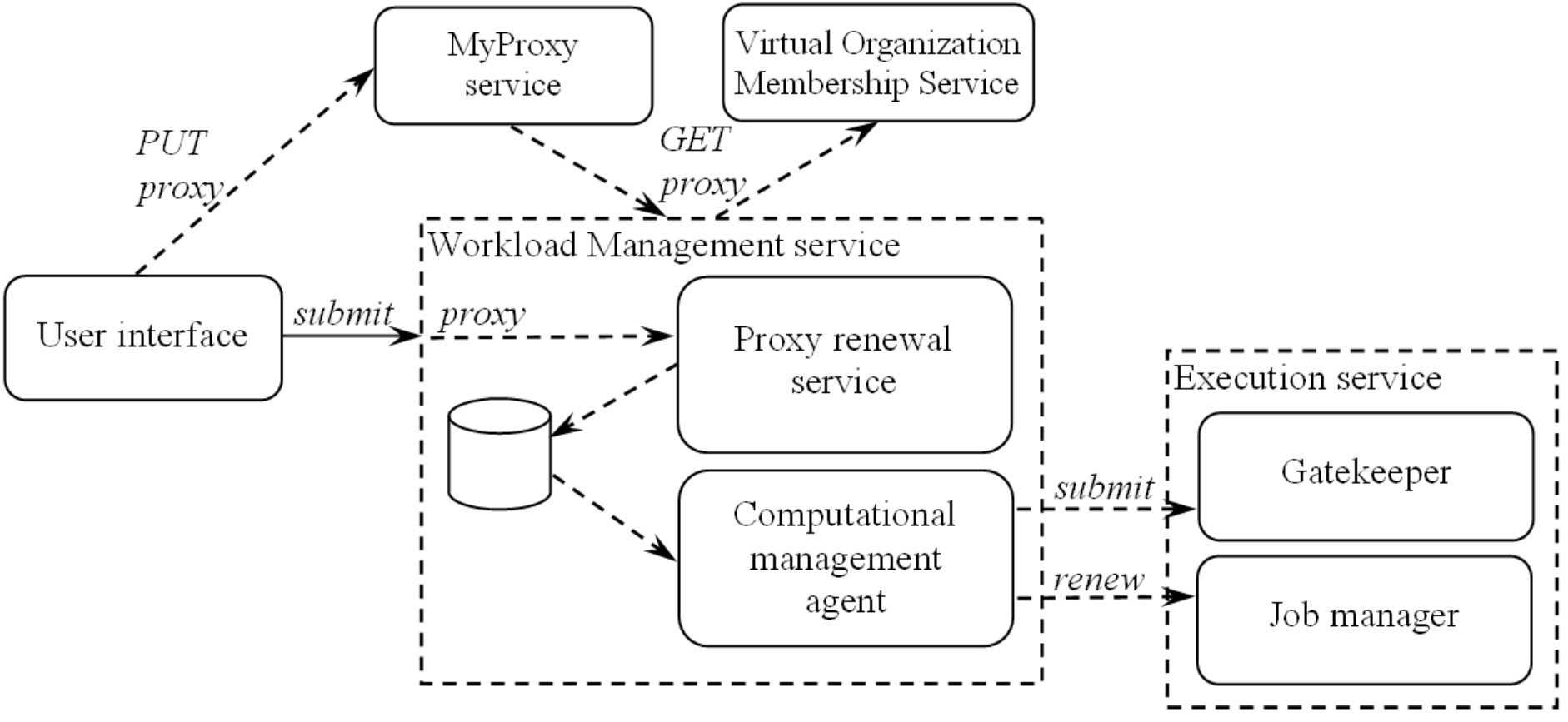
- We will consider a DCS as a set of interacting Web services which send requests to each other.
- One of the most important parts of the DCS is a security infrastructure that provides: authentication and authorization, data integrity, encryption and so on.
- Information security is particularly important in such areas of science and technology as medicine, biological research, and engineering development.
- On the one hand, researchers need to be sure that the results of data processing and simulation are protected from unauthorized access.
- On the other hand, owners of the computational resources that make up the DCS want to have guarantees that only the authorized users will be able to submit computational requests to the system.

Security in Distributed Computing System (2/3)

- The security infrastructure for the DCS is to provide users with a comfortable and secure access to the remote resources. Currently in most DCSs security is based on the PKI in conjunction with proxy certificates. Proxy certificate is a special short time living certificate used for the purpose of providing restricted rights delegation within a PKI based authentication system. In DCSs proxies are used in several cases:
  - To grant the rights between users and services to access to computing resources.
  - While processing a composite computational task. A composite task is a regular task that needs to be processed by several services successively. In this case rights delegation between services takes place.

Security in Distributed Computing System (3/3)

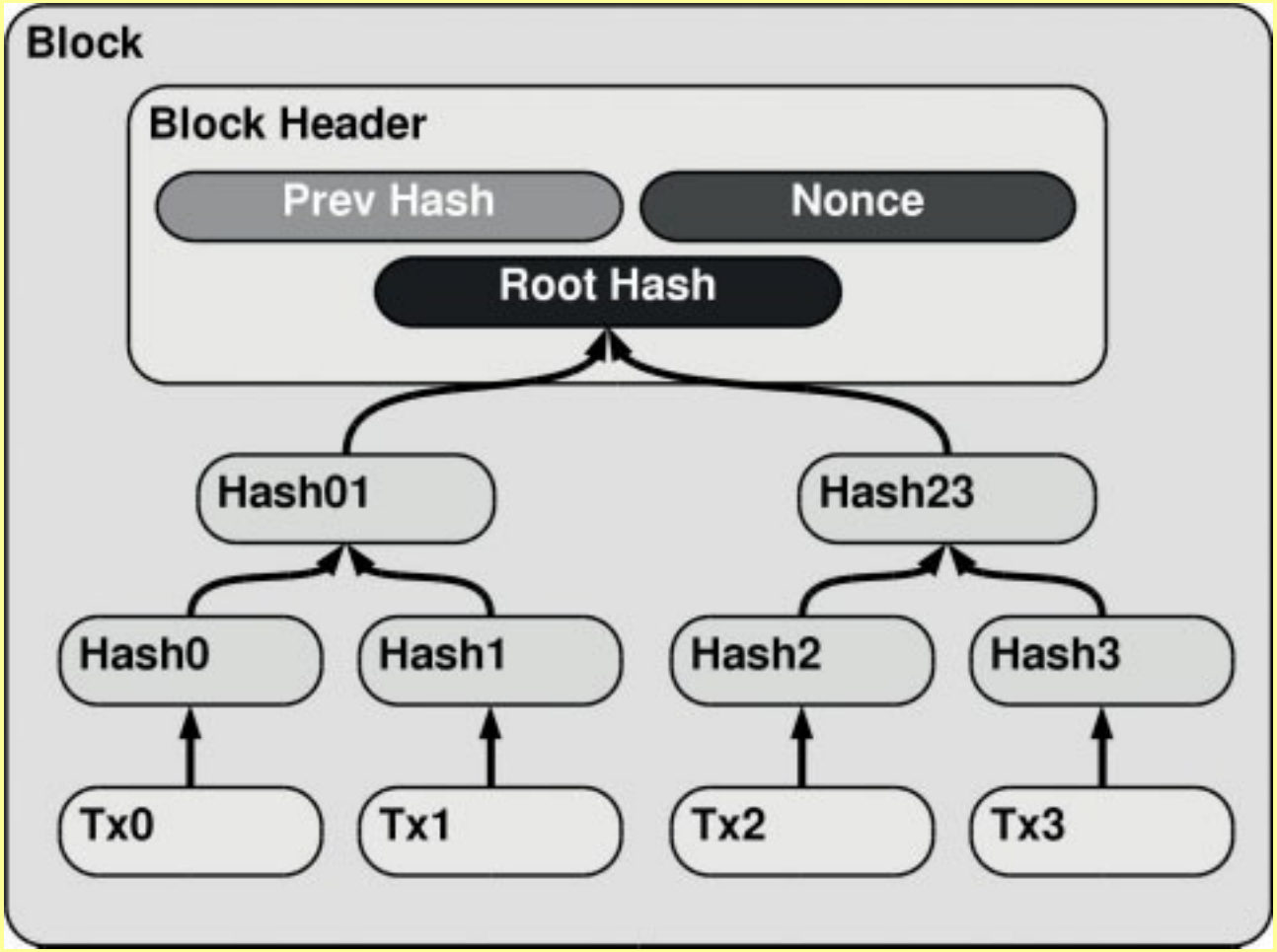
The standard security infrastructure of EGI/WLCG with proxy renewal procedure.



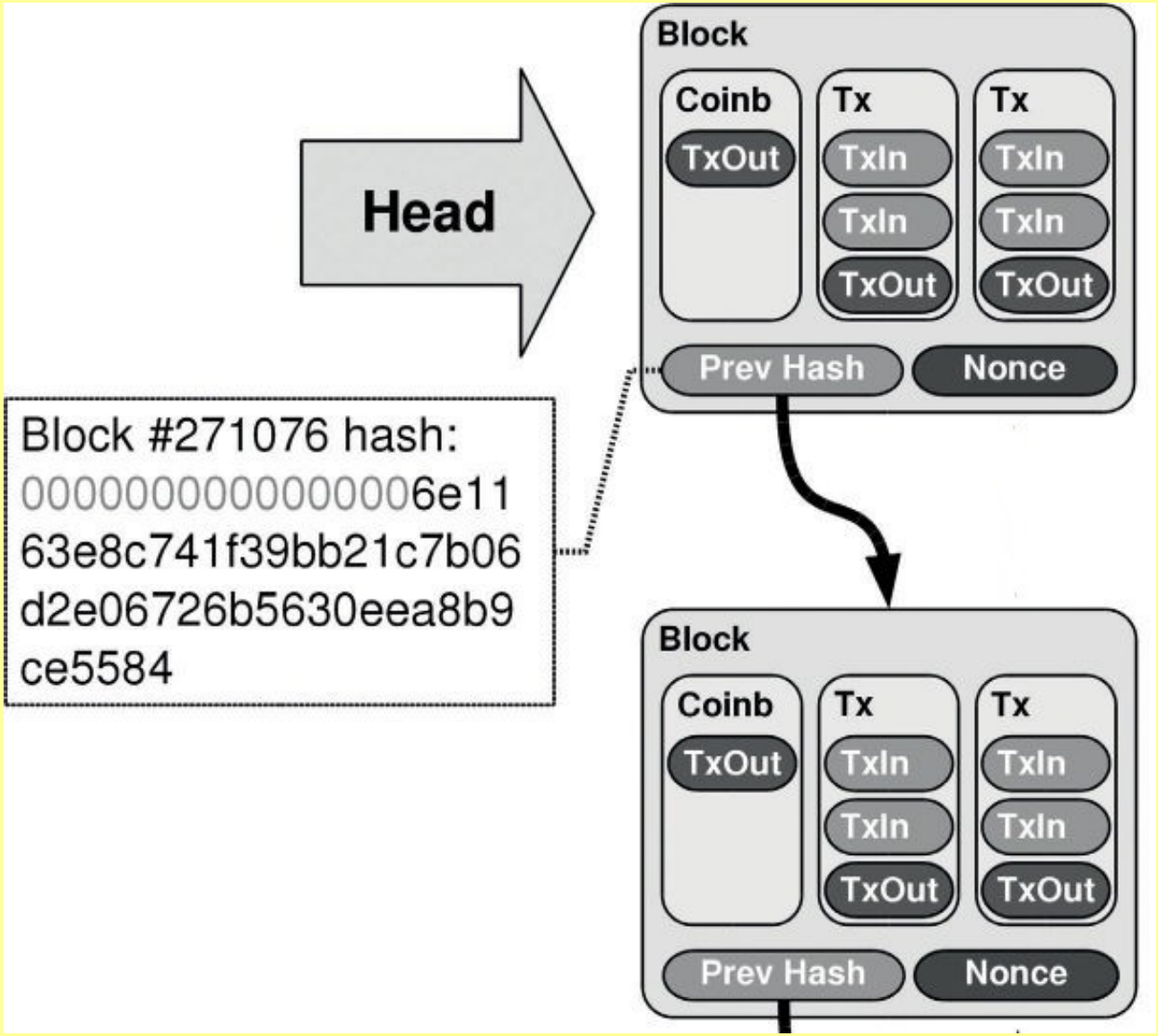
Blockchain technology

- The blockchain became famous in connection with the development cryptocurrency Bitcoin. This is one of basis technology which can use in many IT fields. It is arguably the most important innovation introduced by Bitcoin.
- The main features of blockchain are the following.
  - Hash functions as the cryptographic primitive.
  - Time-stamping is a way to secure information at a certain point in time.
  - The proof-of-work concept.
  - Smart contract.

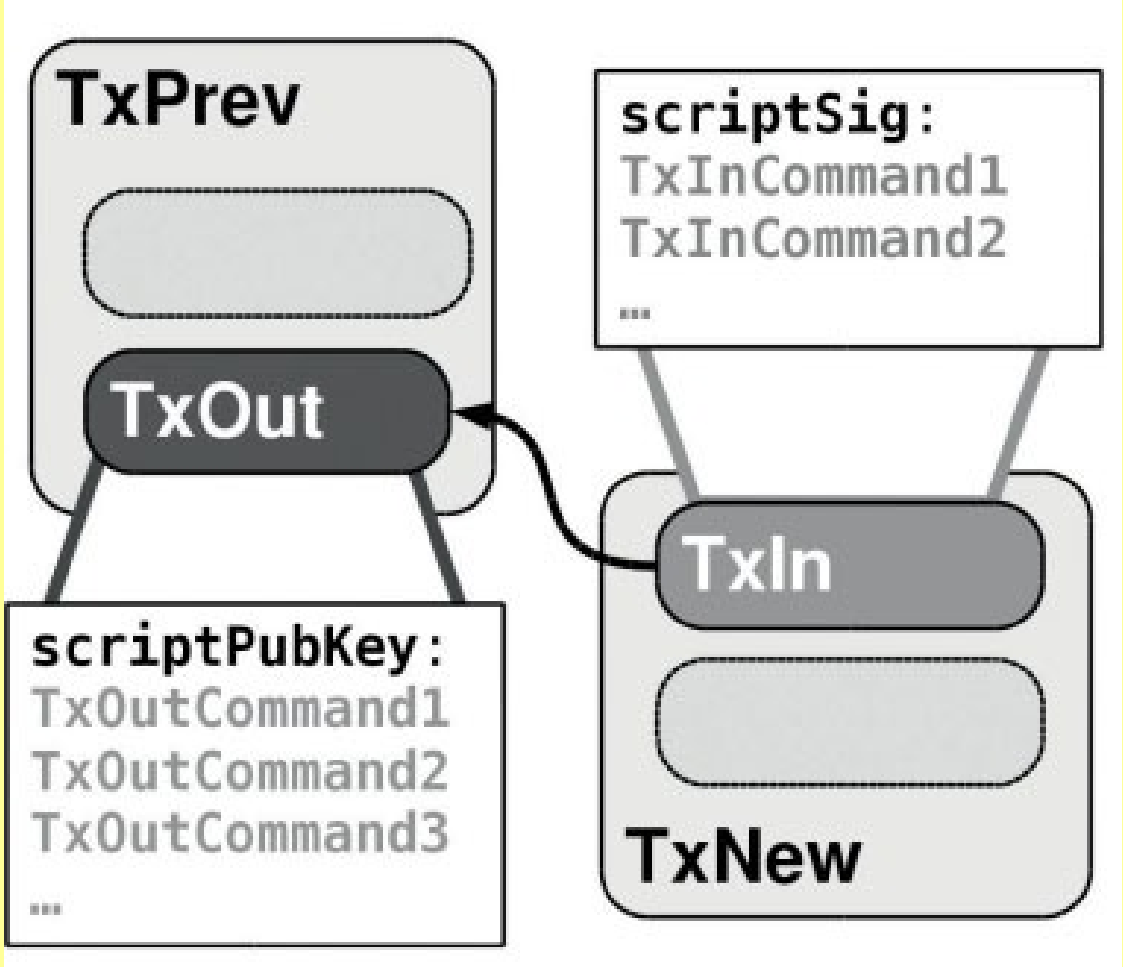
Hashing: Merkle trees

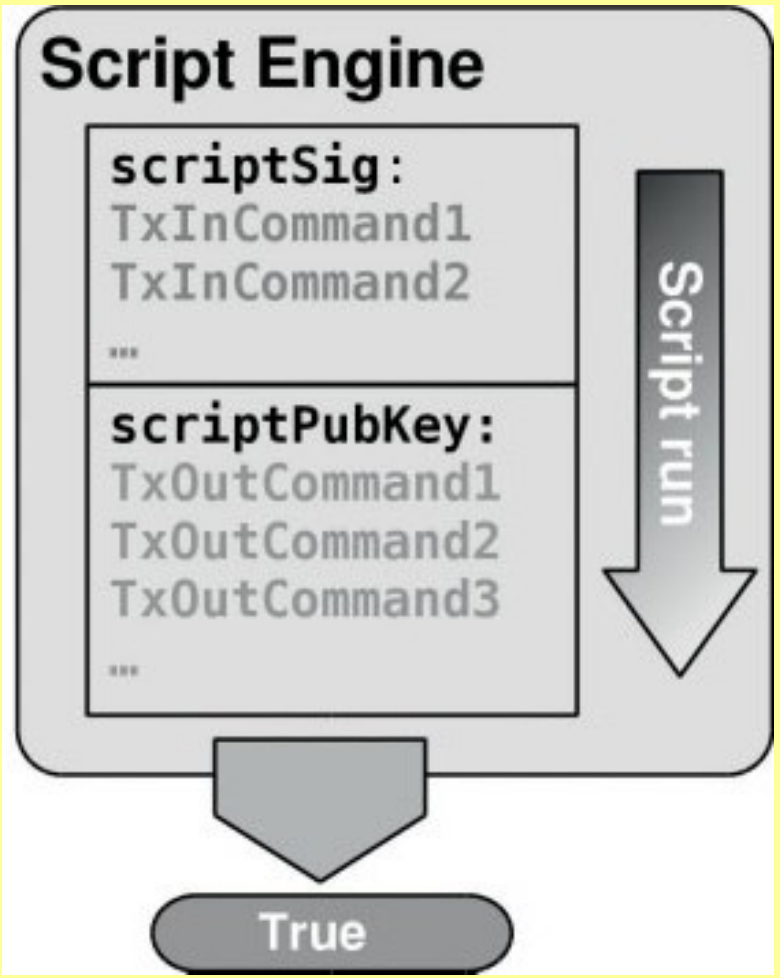


Structure of the blockchain



Smart contract





Ethereum

- Ethereum is an open source second-generation distributed ledger with an associated Turing-complete platform
- Ethereum will create its own blockchain.
- Now the project is still being built, although the test network is up and running.

Applications of contract mechanism in Ethereum

- Digital assets, such as other virtual currencies, application coins, metacoins 20 , and so on.
- Derivatives, such as contract for differences. In fact, any derivative payoff function could be programmed into a contract.
- Multisignature escrows. These are possible with Bitcoin, but the flexibility of Ethereum contracts allows more complex rules.
- Digital assets and applications that can take advantage of Ethereum memory store.
- Decentralized exchanges.
- Decentralized data storage. This would require a separate network specialized in data storage.

Applications of contract mechanism in Ethereum

- Decentralized identity and reputation server. Users can register their pseudonyms in an Ethereum contract that could then be queried by other applications.
- Offering bounties for solutions to computational problems.
- Autonomous agents. The code defining the autonomous agent could be distributed among several contracts that could call one another. Autonomous agents could then be built using different pieces—contracts—that coordinate to perform a complex task.
- Asynchronous multisignature escrow. Users send their partially signed transactions to the blockchain, instead of having to communicate offline as in Bitcoin.

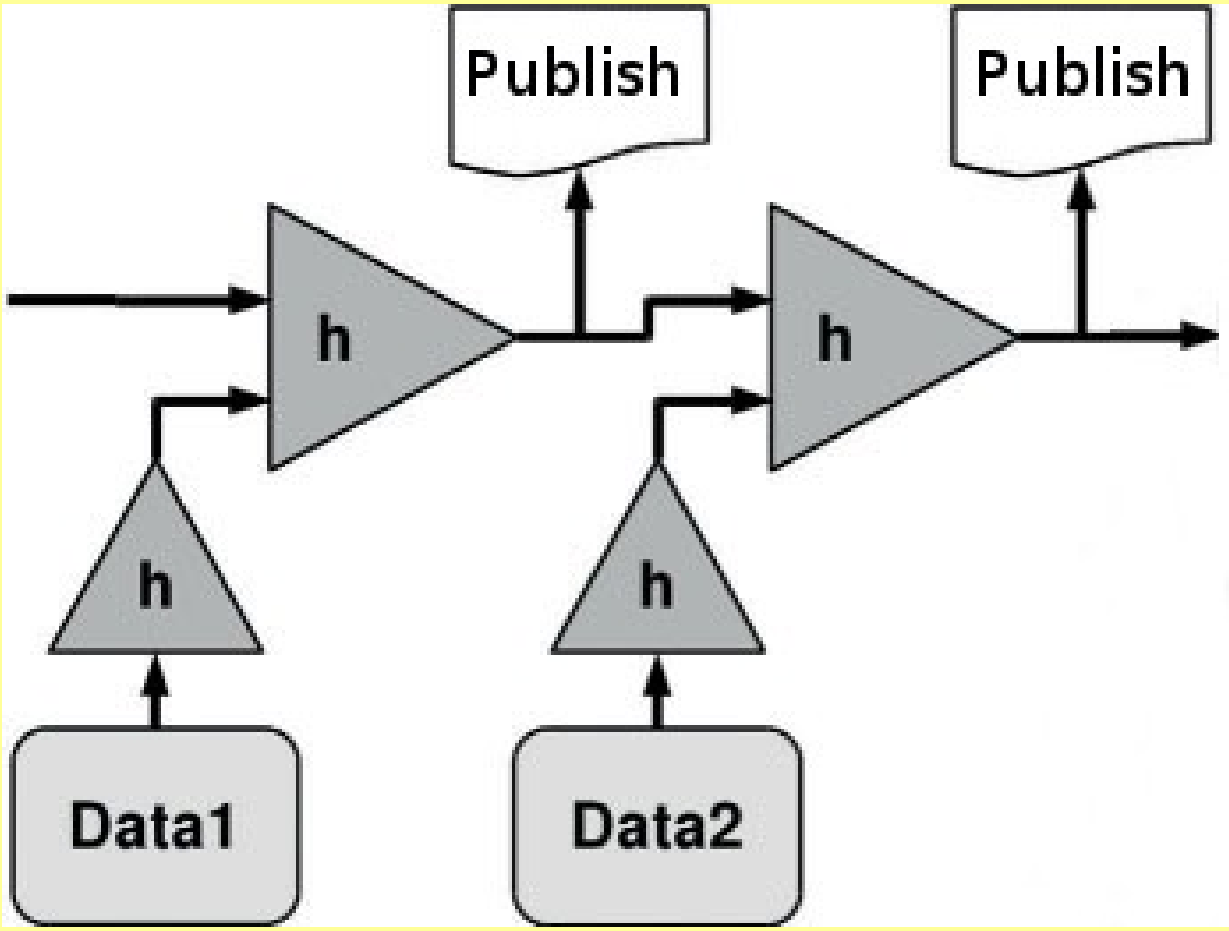
Blockchain In security infrastructure of DCS

- In existing prototype of security infrastructure of DCS we use resticted realization of the blockchain. Taking inti account a specific of DCS we use the following features:
  - Hash function as a primitive cryptographic function
  - Linked time-stamping
  - Smart contract as a preconditions for execution

Hash function

- One-wayness (preimage resistance). Given the hash value, it must be computationally infeasible to find out the input data.
- Weak collision resistance. Given an input it is computationally infeasible to find another input with the same hash value.
- Strong collision resistance. It is computationally infeasible to find two input data points that result in the same hash value.
- Currently we use SHA-256.

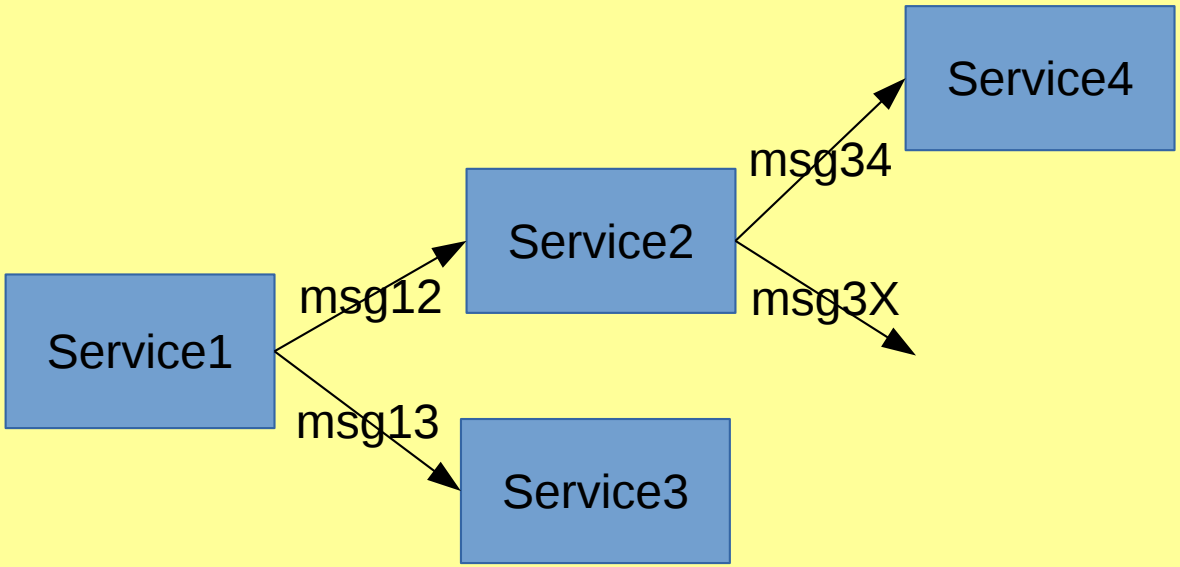
Linked time-stamping

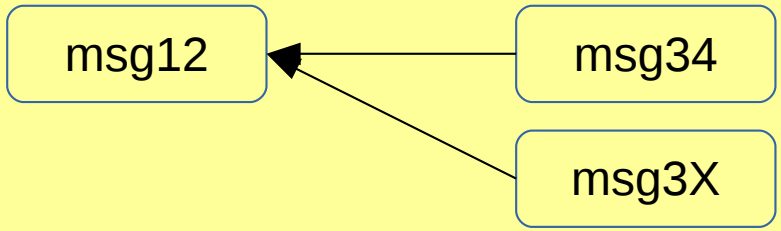


Blockchain In security infrastructure of DCS

- DCS is a set of (Web-) services interacting by messages to each other.
- Any services may generate secondary messages to complete processing.
- All message should be signed by creators to protect it from unauthorized modification.
- All messages should contain time-stemp.
- Use smart contract for specific request like multiple signature.
- So, the messages form chains which we will consider as a blockchain.

Blockchain in security infrastructure of DCS





- Answer we consider as a new messages in reverse direction

Structure of the message

Current prototype of the message consists of:

- {msg_id,linked_time-stamp}
- {owner_id,auth_url,signature}
- {source_url,parent_msg_id,scontract_in}
- [{destination_url, msg_body,scontract_out}, ...]
- merkle_hash

- You can use encryption to protect message content.

DCS blockchain vs. classical one

- The main difference between DCS and classical blockchain are:
  - We do not use the proof-of-work concept.
  - We do not support anonymous access to the DCS
  - The group of users can deploy special authorization service which will support the authorization process for the group.
    - In some sense this is reincarnation of the central service. However, the idea is that the group (~ VO) can deploy this service independently of the other. This is just one of the other services in the DCS.

Conclusion

- In this work, we investigate the possibility of abandoning the special dedicated servers in the DCS security infrastructure and the use instead of them a distributed database on the basis of the blockchain technology, the paradigm of smart contracts, maybe using Ethereum protocol.
- Since in this case the database of the security infrastructure is distributed across all the nodes in the system, this approach will increase the resiliency and security of DCS.

Thank you for attention!