Complete decentralization of distributed data storages based on blockchain technology

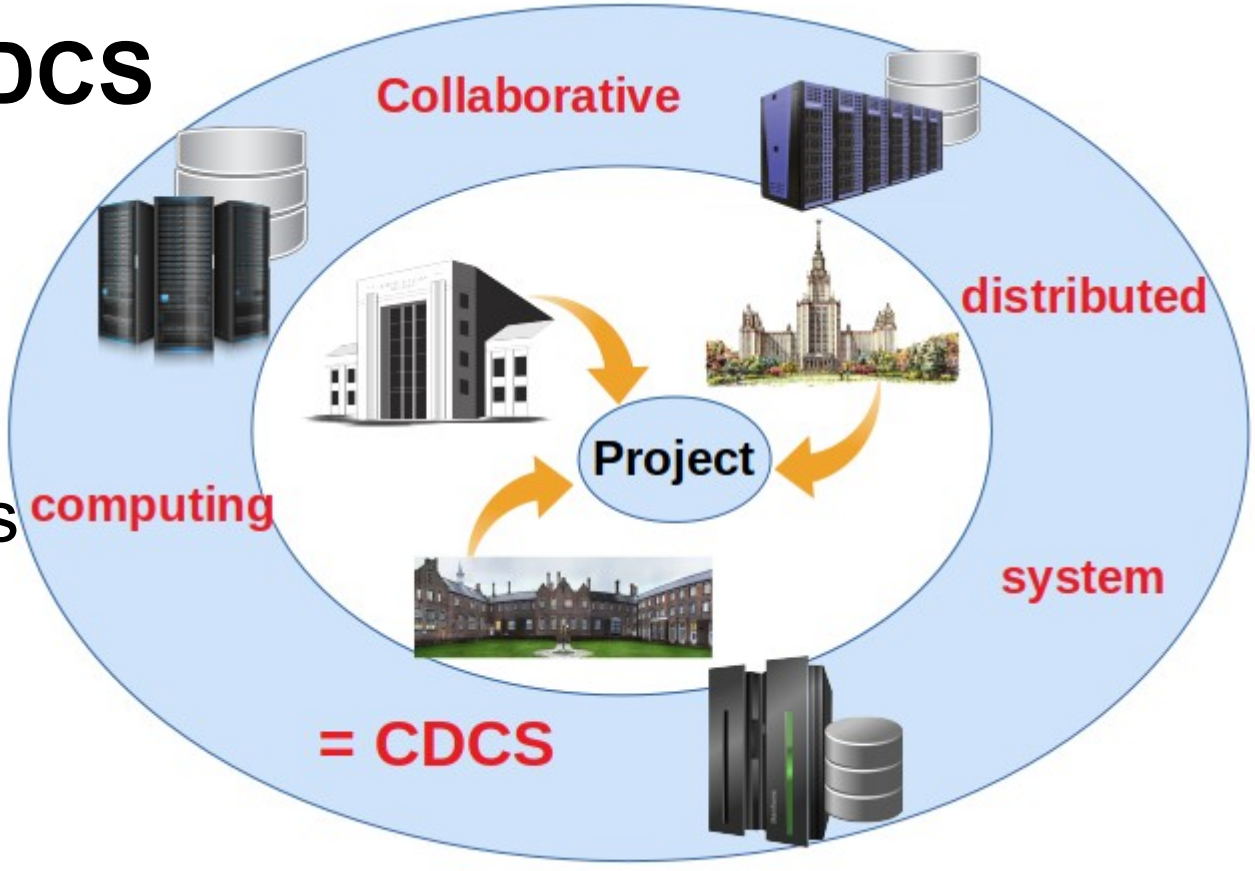
A. Demichev and A. Kryukov

SINP MSU

Supported by RSF grant No. 18-11-00075;
R&D State Assignment No. 115041410196

Collaborative DCS

- organizations participating in a large project integrate their local computing resources into a unified distributed pool
  - administratively unrelated user groups share computing resources based on an agreed policy



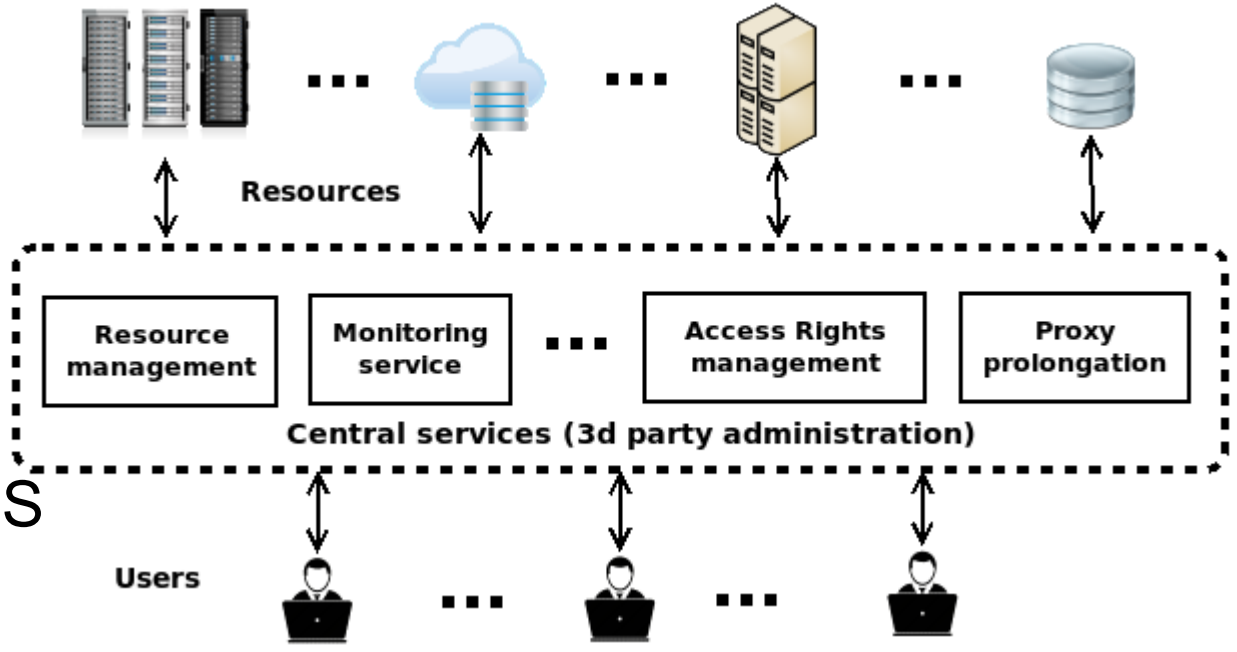
- partial or complete lack of trust between user groups
- dynamically changing distributed environment

Typical structure of a CDCS

- **distributed** resources are combined into a single pool using the infrastructure based on **centralized** services

- layer of user interfaces
- layer of resource sites
- layer of system-wide

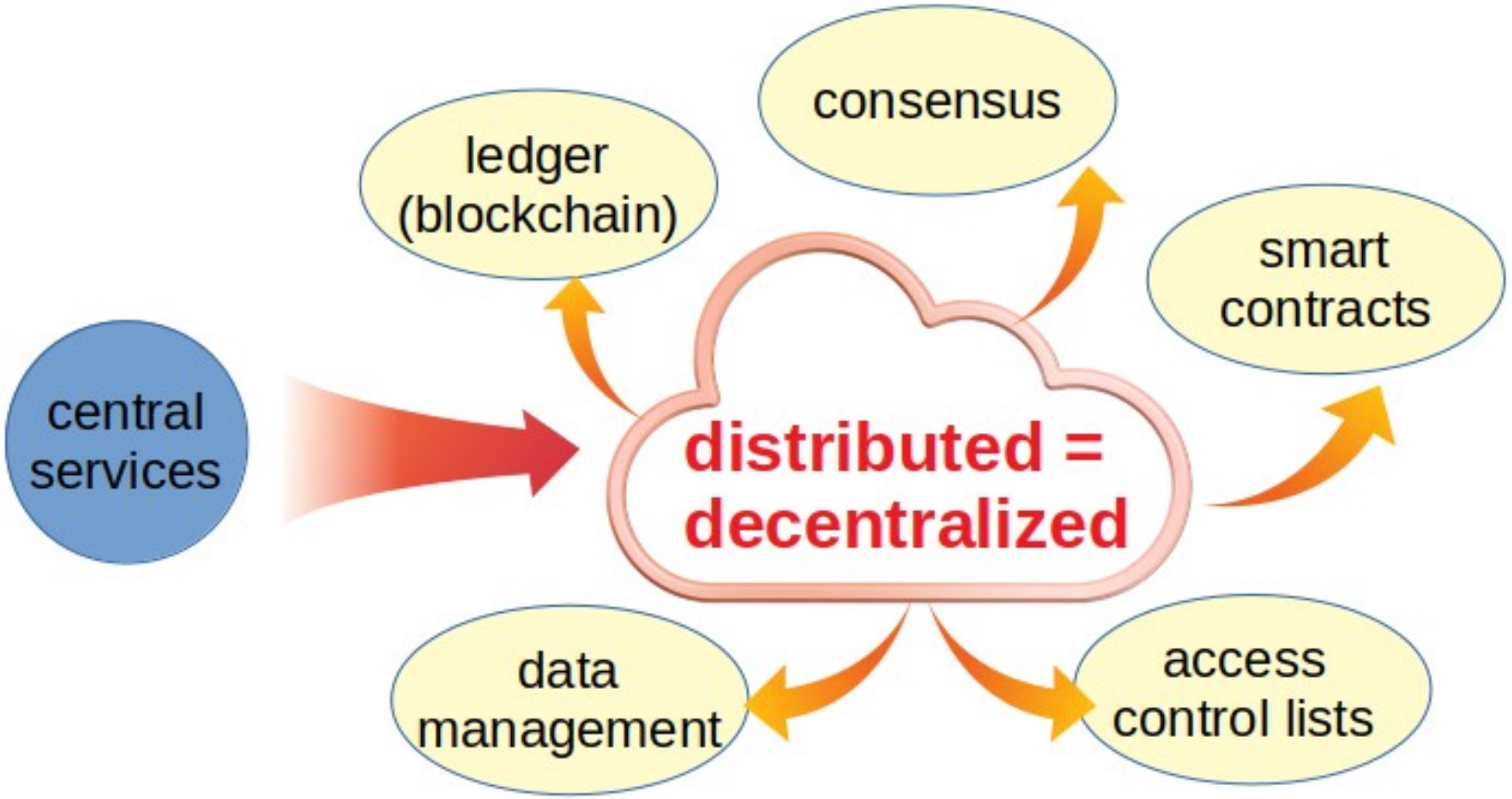
centralized services that manage the work of CDCS as a whole



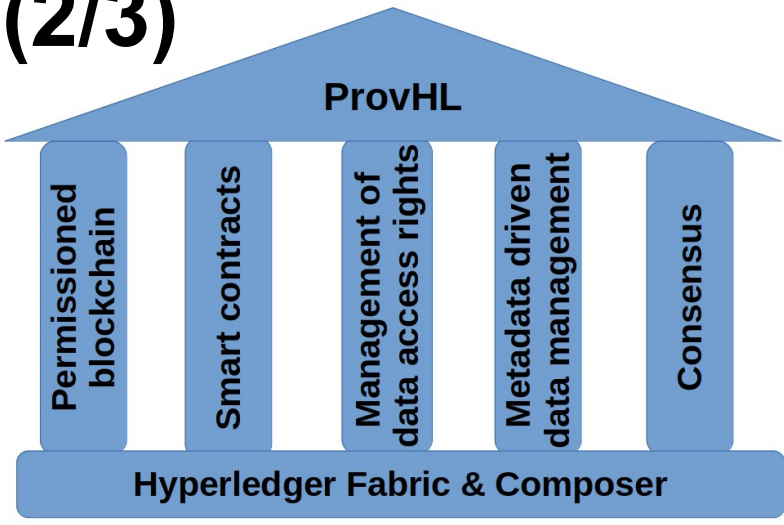
→potential **points of failure**, malicious intrusion and/or bottlenecks

→users have to trust 3d party administrators

Approach to Decentralization (1/3)

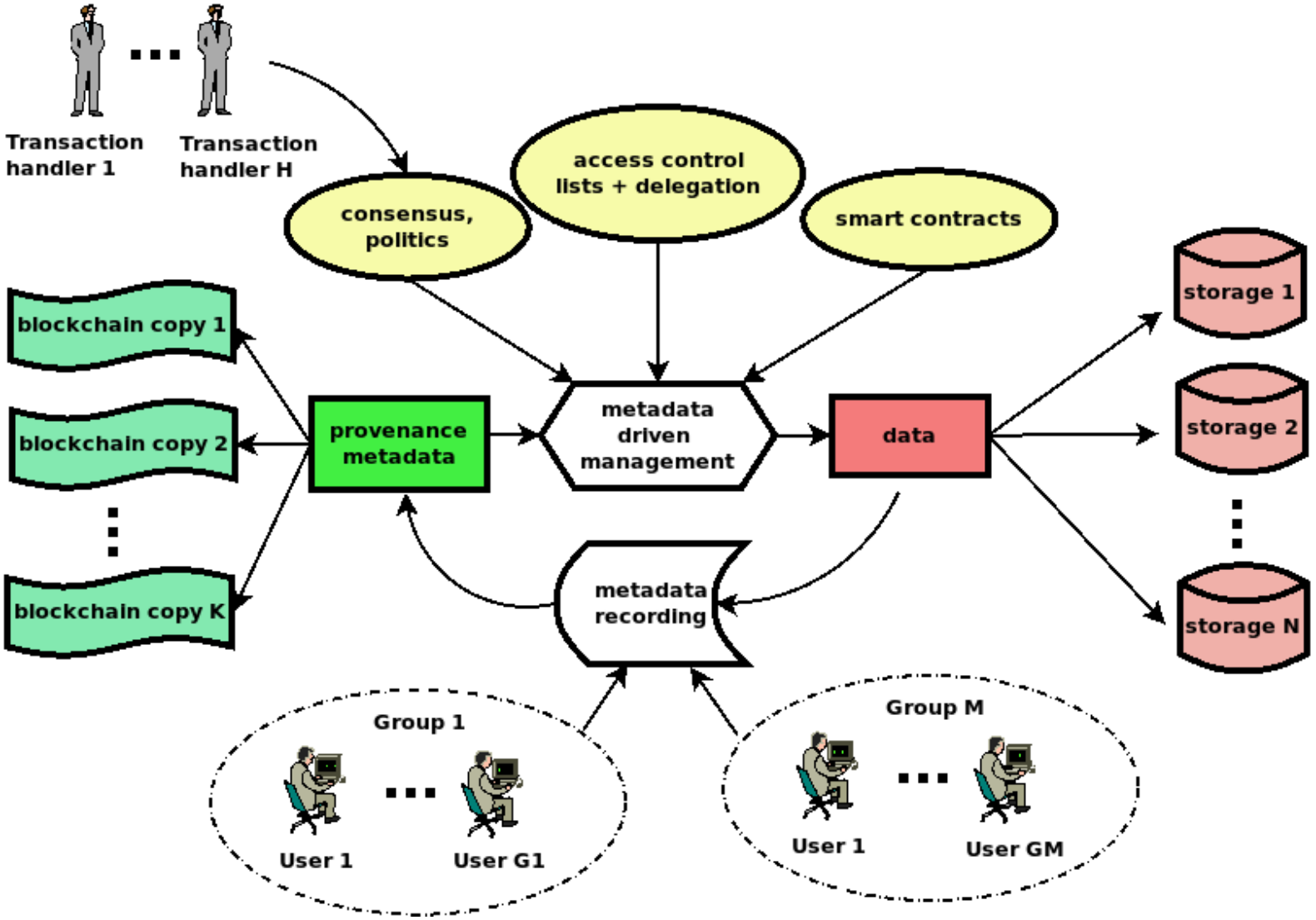


Approach to Decentralization (2/3)



- built upon the integration of the following solutions:
  - use of a distributed ledger based on permissioned blockchain;
  - use of smart contracts
    - defines rules of data sharing in CDCS in the form of executable code
  - metadata driven data management;
    - provenance metadata (system history) are written to the blockchain in advance, and data management system accesses the blockchain and performs the transactions recorded there;
  - consensus between representatives of the parties in the data sharing process
  - distributed ACL & delegation.

Approach to Decentralization (3/3)

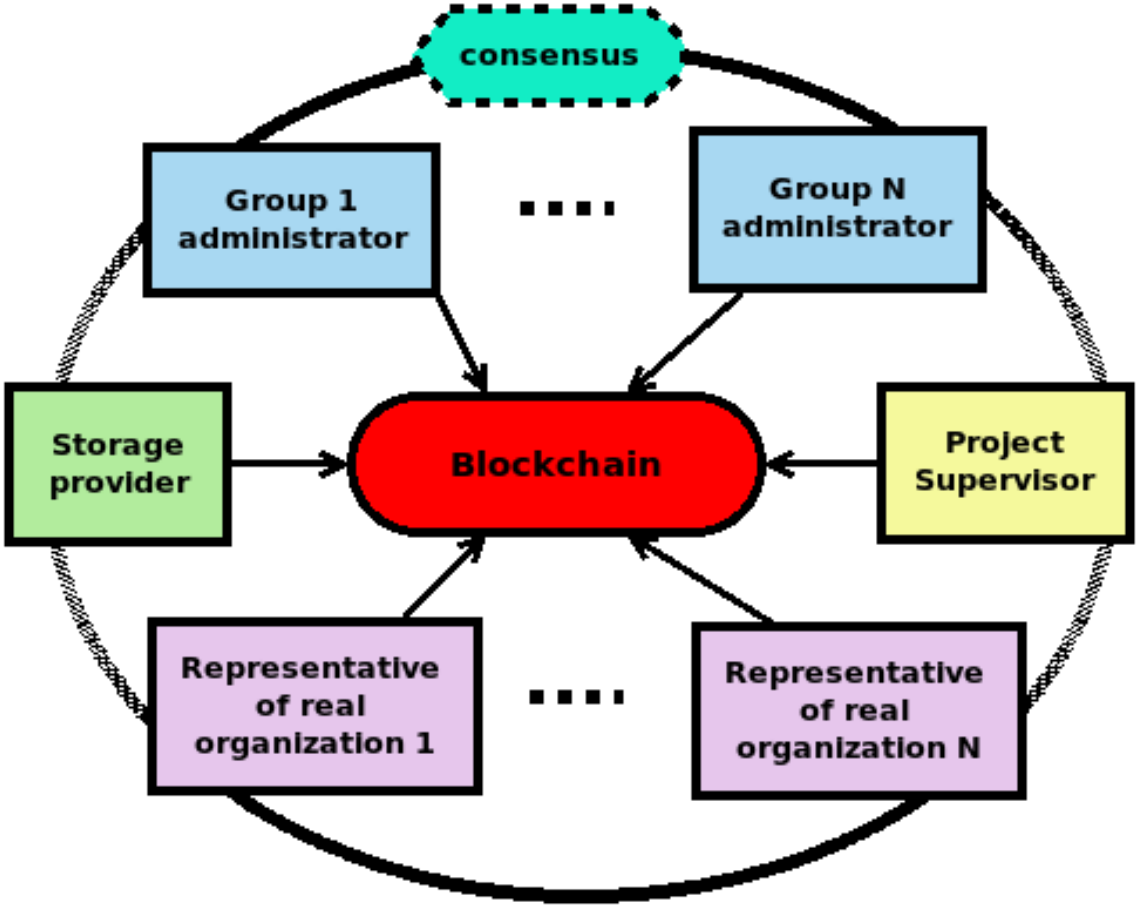


The Approach Implementation: ProvHL

- **ProvHL** = Provenance HyperLedger
  - based on the Hyperledger Fabric (HLF) blockchain platform (*hyperledger.org*)
  - adaptation of HLF for the business process of sharing storage resources
- state of the entire CDCS recorded in the blockchain= aggregated state of the files=metadata
- **permissioned blockchain**:
  - immutable records of history of all activities
  - transactions are processed by **specified entities**
- **more controlled** and predictable environment than public blockchains + much **better performance**

Examples of Transaction Handlers in Collaborative DCSs

Permissioned BC: suitable for networks with naturally existing trusted entities for the transaction processing



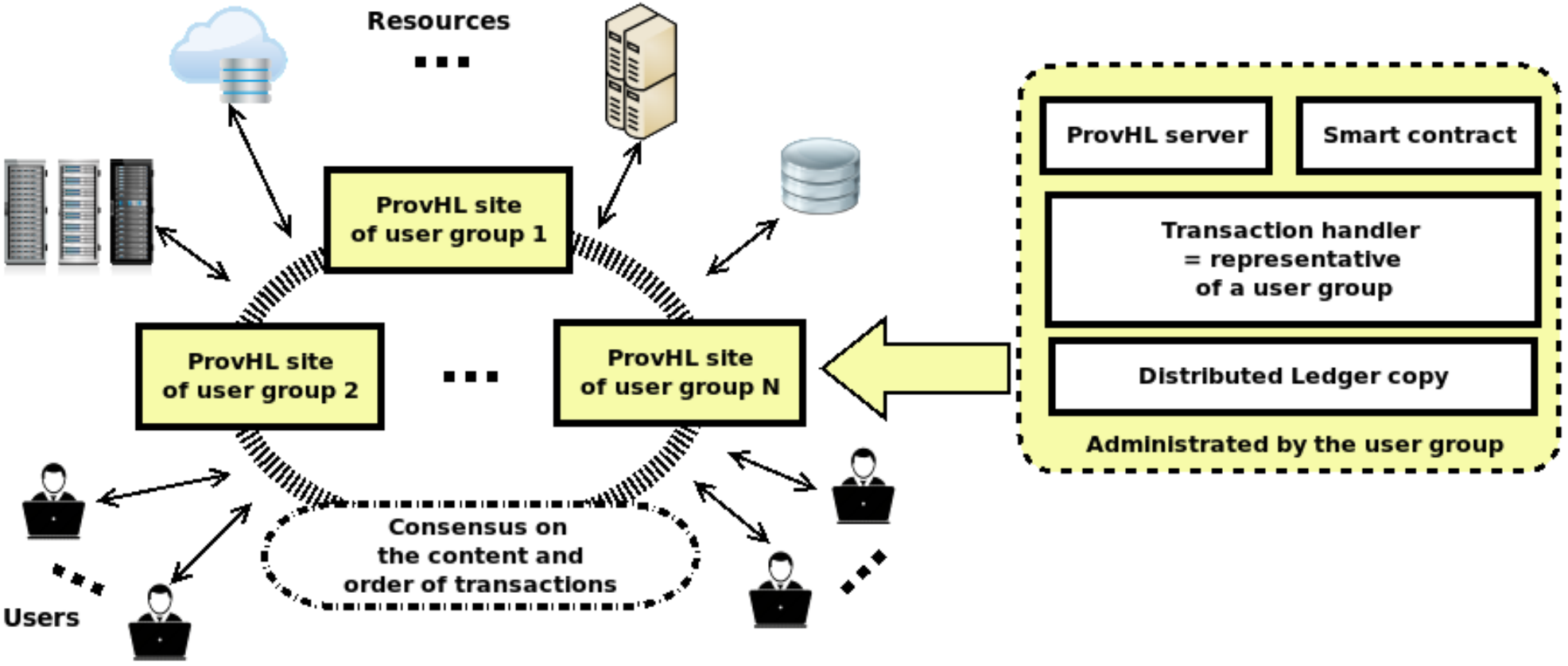
the handlers must come to a **consensus** about the content and the order of the recorded transactions

this is achieved via **distributed** consensus algorithms

Consensus in Hyperledger Fabric/ProvHL

- Transaction **endorsement**: endorses the transactions by simulating the transaction execution process
- **Ordering**: set of ordering services take endorsed transactions and decide on a sequence in which the transactions will be written to the ledger
  - Ordering Consensus Algorithms
    - SOLO, Raft, Kafka, BFT,...
- **Validation and commitment**: committing peers first validate the transactions received from the orderers and then commit that transaction to the ledger

General Structure of a Collaborative DCS under ProvHL Management

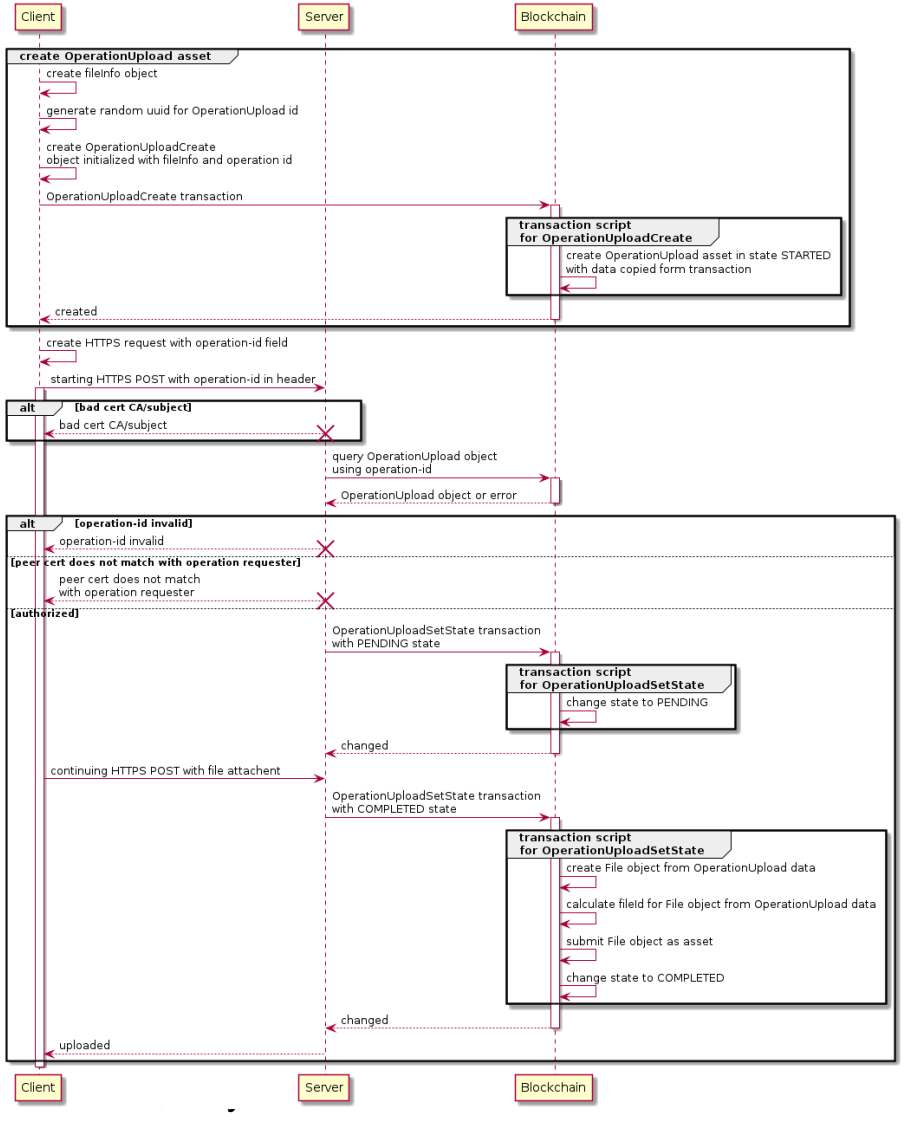


ProvHL: Basic operations ⇒ transactions

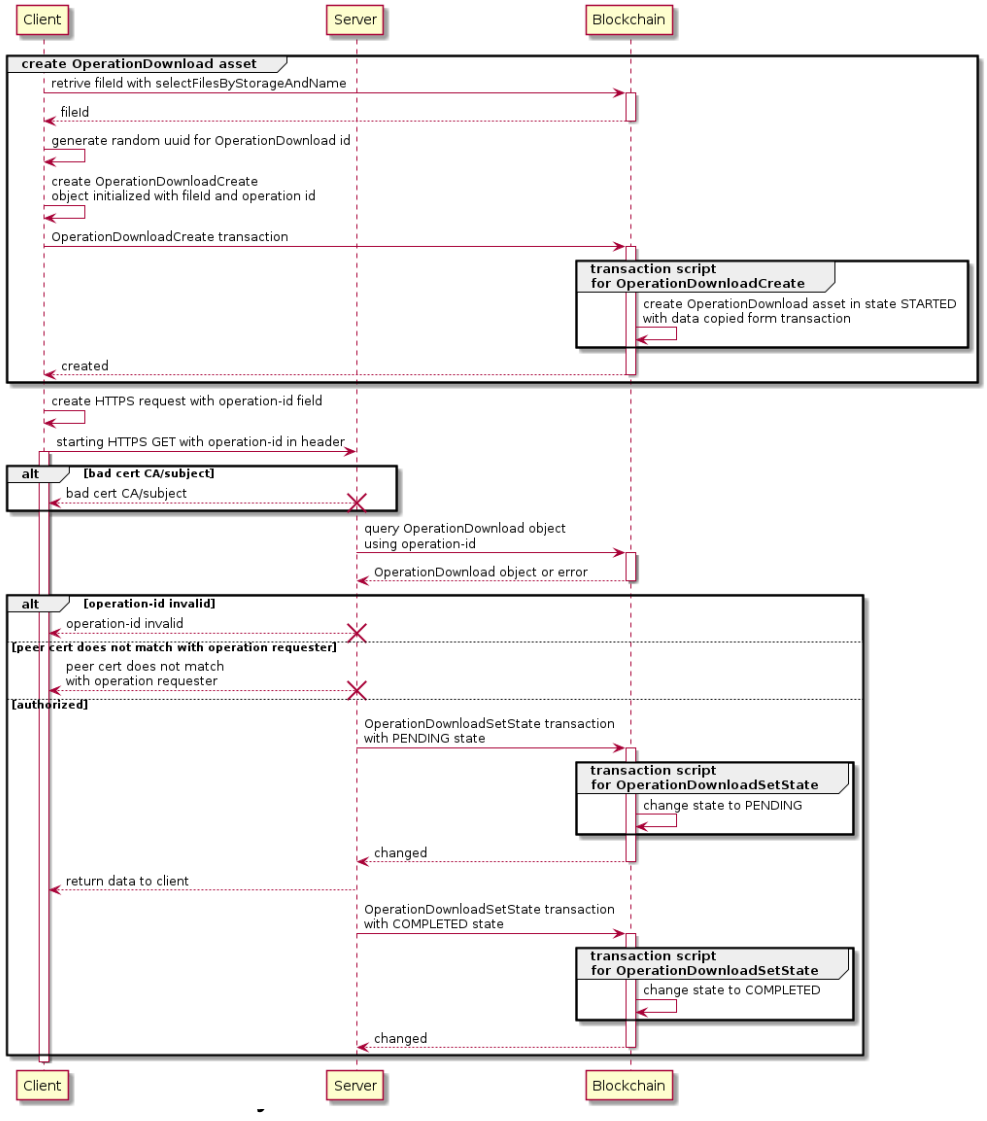
- new file upload
- file download
- file deletion
- file copy within local storage
- file copy/transfer to another local storage
- file transformation by a special service ⇒ grid-like DCS
  - each operation comprises of a number of transactions
  - each valid transaction ⇒ update of some state attributes
    - for example, after the transaction "file download" the values of the keys change: "number of file downloads" and "users who downloaded the file".

Sequence Diagrams

Upload



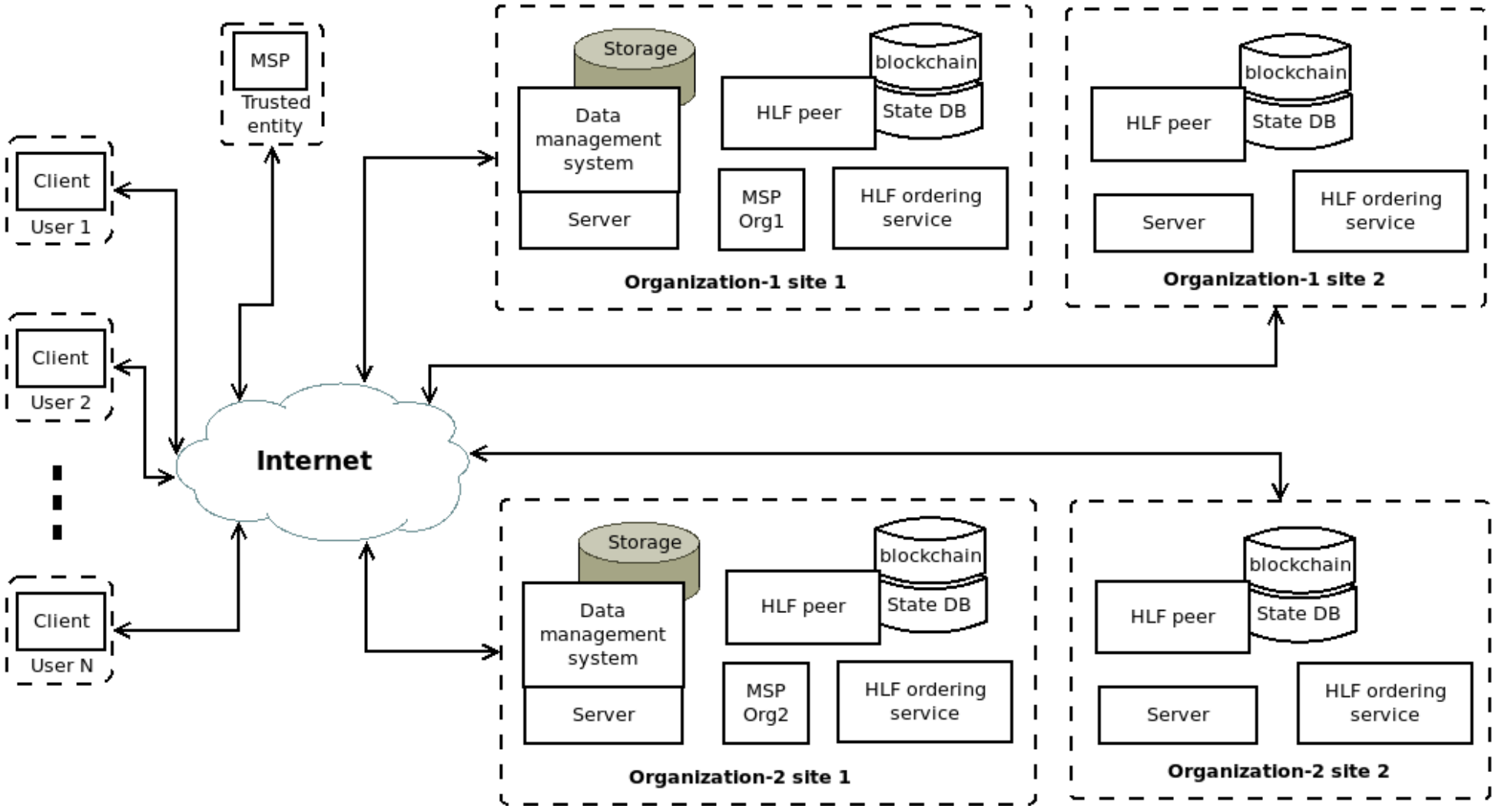
Download



Further ProvHL Features

- **Decentralized:**
  - user group management
  - access rights management
    - on the level of users or user groups ⇒ well-structured management of access rights
    - including rights **delegation**
      - without proxy: all the info about delegation process is recorded into the distributed ledger
  - management of virtual (overlay) directories throughout the CDCS

ProvHL Testbed



Performance Characterization of HLF & ProvHL

- HLF
  - for the input transaction rate up to 800 tx/sec, the transaction latency is ≤1 sec
  - transaction throughput is ~ 800 tx/sec
- ProvHL (each file operation consists of 3 ÷ 7 transactions)
  - ⇒ matching results for the latency ~ 4 ÷ 7 sec
  - throughput ~ 100 ops/sec.
- quite acceptable for operations with files of sufficiently large volumes
  - typical for DCS for large scientific experiments

Conclusion (1/2)

- we have suggested the new approach to the safe and secure metadata driven data management in CDCSs based on the integration of
  - blockchain technology
  - smart contracts
  - metadata driven data management
  - consensus algorithms
- intended for operation in a **distributed environment** with administratively unrelated organizations participating in joint projects
  - conditions of **incomplete trust or lack of trust** between groups of users of the system

Conclusion (2/2)

- ProvHL system on the top of Hyperledger Fabric blockchain platform
  - **completely distributed/decentralized** ⇒ fault-tolerant
    - free from the vulnerabilities associated with the presence of central services which can be bottlenecks and points of failure
  - well granular access control management
    - including delegation of rights
  - testbed performance characteristics are promising
  - more details: Demichev, Kryukov & Prikhod'ko "Business Process Engineering for Data Storing…" **Journal of Grid Computing** (2021); 19(1):1-30.