A Design of Blockchain-based Architecture for the Security of Electronic Health Record (EHR) Systems

Guang Yang, Chunlei Li

Western Norway University of Applied Sciences,

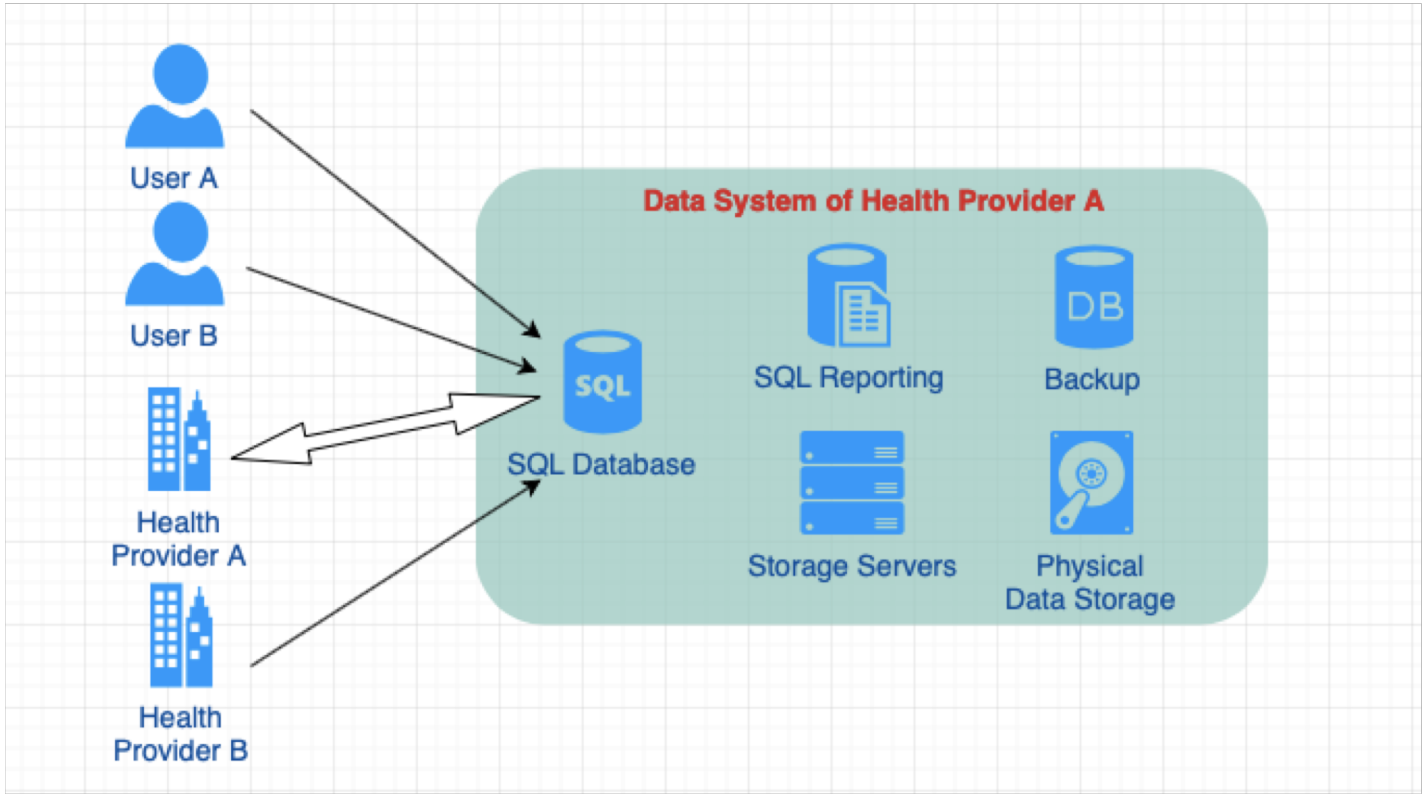
and University of Bergen, Norway

Outline

- Introduction and Background
- System Overview
- Implementation of the Blockchain
- Discussion and Summary

Introduction and Background (1)

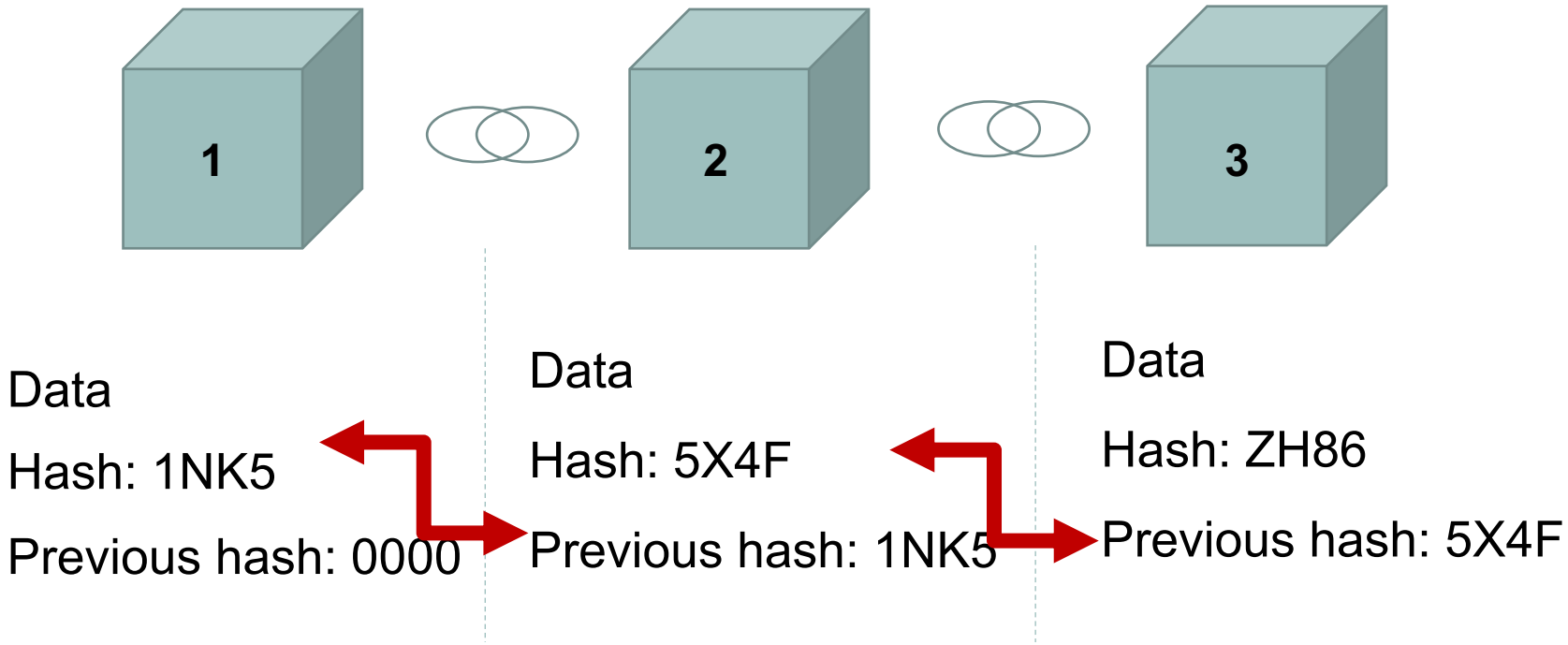
- The Norwegian national health system
- The Norwegian national electronic health record system



Challenge !

Introduction and Background (2)

- Block: data, hash, hash of previous block
- Blockchain prevent tempering: hash, proof-of-work, distributed

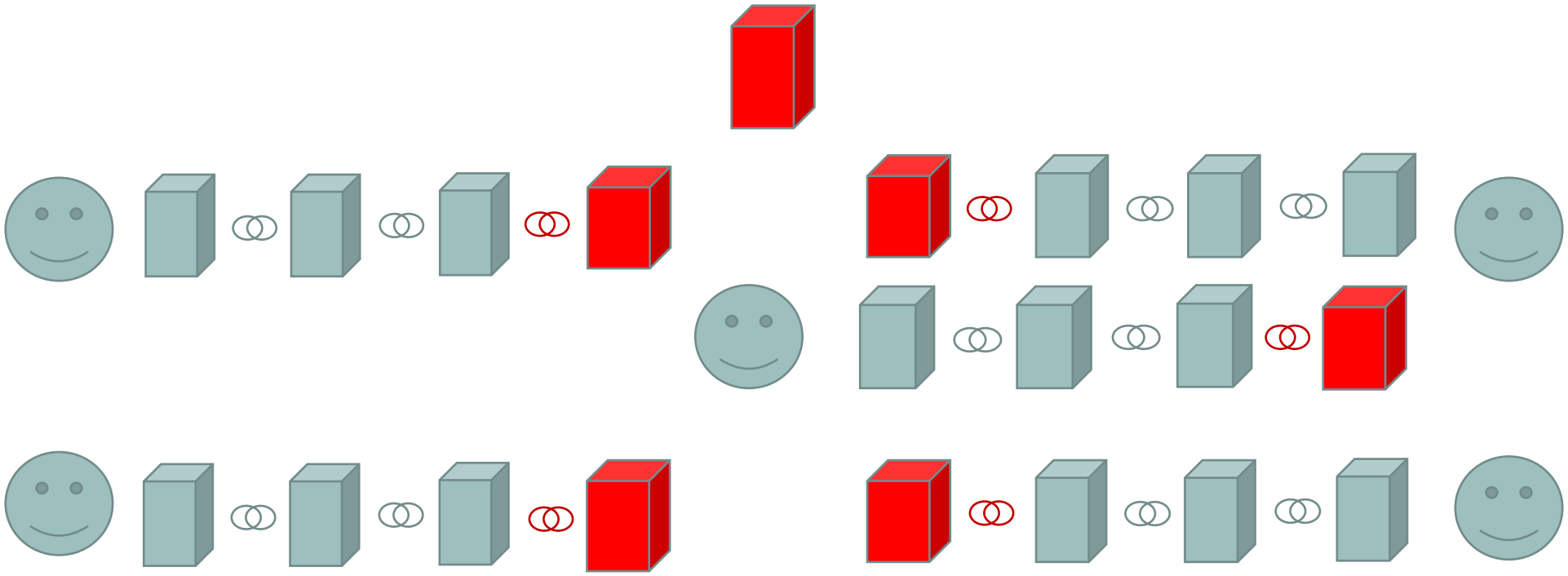


Introduction and Background (3)

- Proof-of-X consensus model

In Bitcoins case: it takes about 10 minutes to calculate the required proof-of-work and add a new block to the chain.

- Distributed



Introduction and Background (4)

Smart Contract

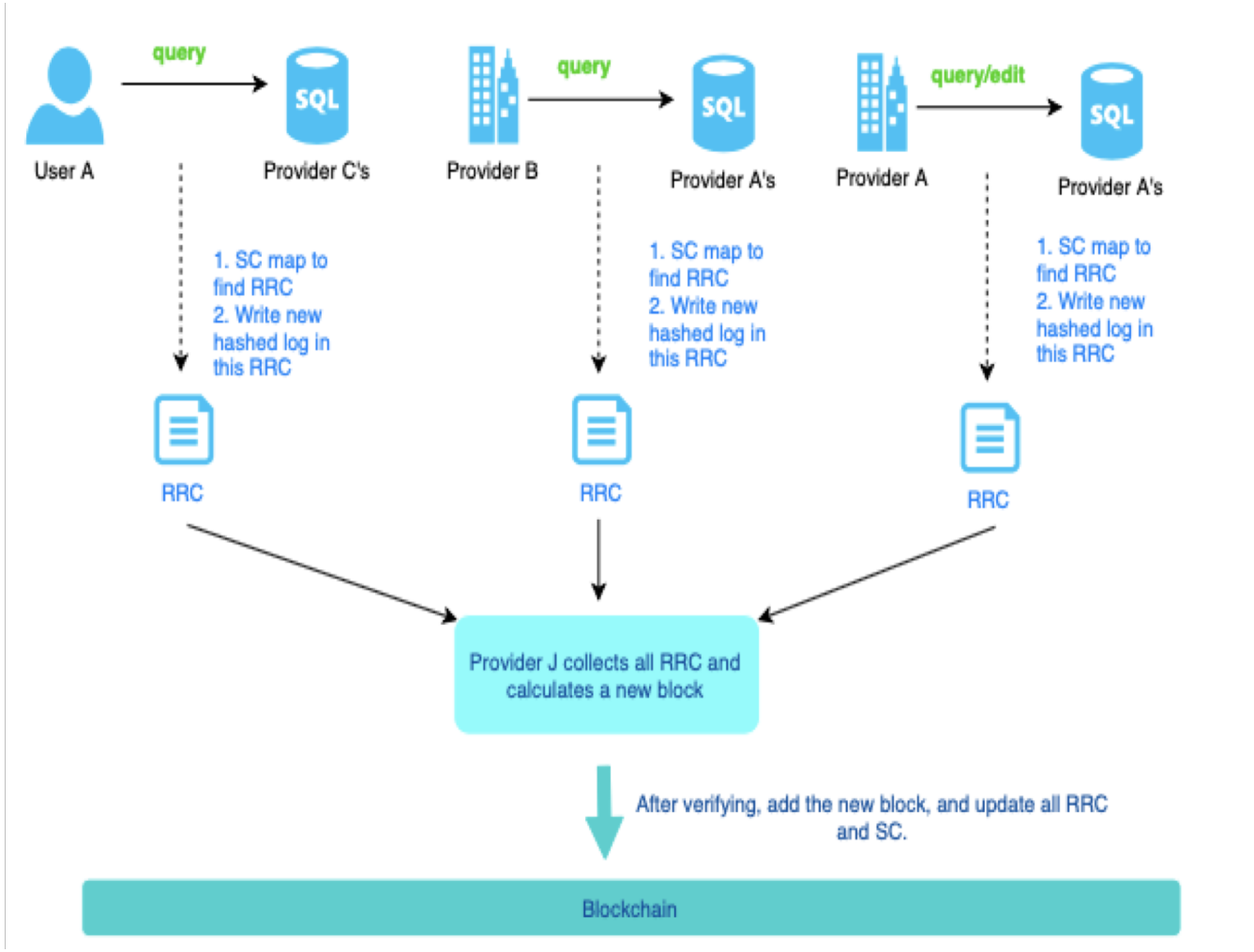
- A piece of computer code that rules relationship of nodes in the network
- Is stored on the blockchain
- Functions among the distributed network
- Execution processes are automated and immutable once have been agreed
- Has been implemented in many blockchain projects,

  e.g. platforms: Ethereum and Hyperledger

System Overview of Our Architecture

- Building on top of the existing providers databases
- The blockchain keeps track of all events that happened to the data in the databases.
- Ownerships and access rights of records are added to the chain.
- *Summary Contract (SC)* and *Record Relationship Contract (RRC)*
- Propose a new incentive mechanism

System Overview



Implementation of the Blockchain

- Initialization: consensus
- ***Significance*** S_i of provider P_i

  suppose P_i has m_i pieces of records in its database.

$$S_i = \sum_{t=1}^{m_i} v_t \,,$$

where, v_t is the value of each record R_t for a user U_t.

Consider completeness $X_{t,\omega}$ and redundancy $I_{t,\omega}$:

$$v_t = \frac{1}{\Omega} \sum_{\omega=1}^{\Omega} X_{t,\omega} \; I_{t,\omega}$$

$$\text{then, } S_i = \sum_{t=1}^{m_i} \left(\frac{1}{\Omega} \sum_{\omega=1}^{\Omega} X_{t,\omega} \; I_{t,\omega} \right)$$

Example of Significance

- P_1, P_2, P_3
- Ω = 32 ($I_1, I_2, \ldots I_{32}$)
- P_1 : 20 records, each has 8 unique items

  thus value of each record is $\frac{8}{32} = \frac{1}{4}$, and the S_1 is: $20 \times \frac{1}{4} = 5$
- P_2: 30 records, 16 items, of which 8 records have duplicated 4 items with P_3,

  thus, S_2 is: $8 \times \frac{1}{32}\left(4 \times \frac{1}{2} + 12\right) + 22 \times \frac{16}{32}$ = 14.5

Implementation of the Blockchain

- Incentive Mechanism

Firstly, we define :

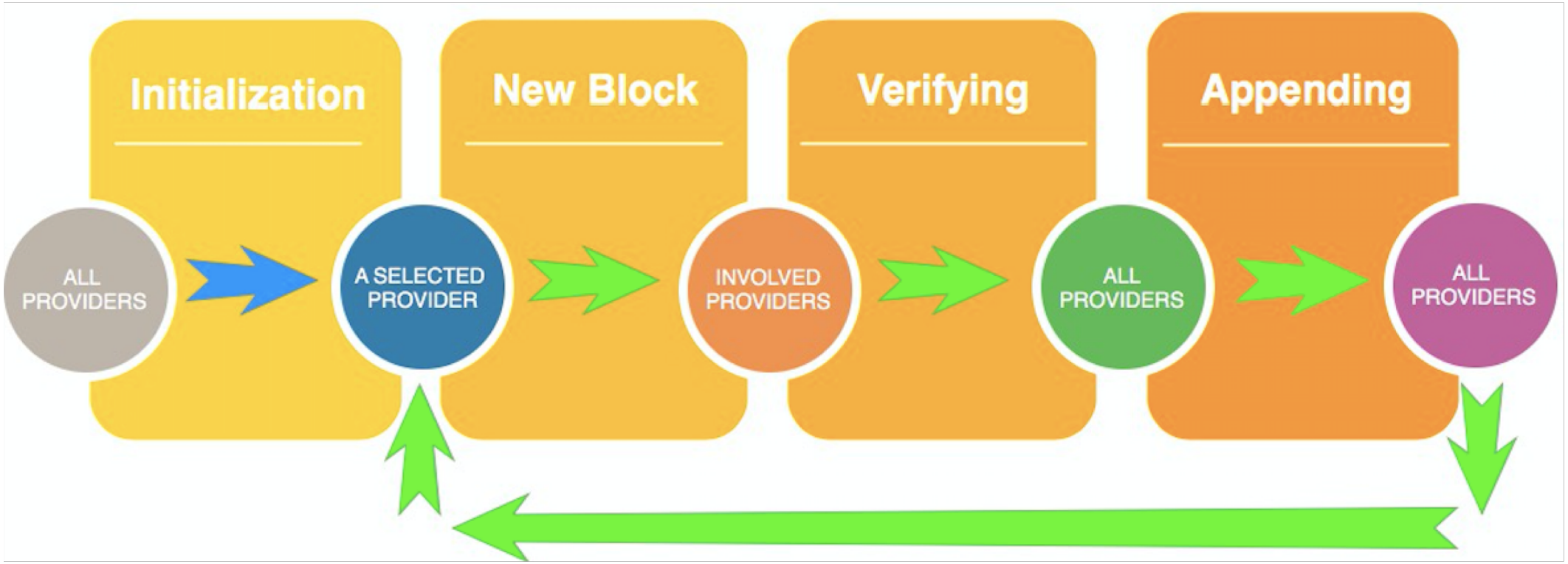
$$p_i = \frac{1}{n-1} - \frac{S_i}{(n-1)\sum_{i=1}^{n} S_i}, \qquad 1 \le i \le n.$$

Then, generate a random number in the range of [0,1), the provider P_j is selected if the random number falls into a range A_j as following:

$$A_j = \begin{cases} (0, p_1), & if\ j = 1 \\ \left[\sum_{i=1}^{j-1} p_i, \sum_{i=1}^{j} p_i \right) & if\ 2 \le j \le n. \end{cases}$$

- After the new block has been verified by other providers, P_j will increase its significance as incentive.

Implementation of the Blockchain



Discussion (1)

- The incentive mechanism
  - Not intend to involve monetary
  - Permissioned blockchain
- The significance
  - From maintaining data and computing new blocks
  - Aiming to achieve a fairness among all providers
- The incentive value
  - Fraction of average
  - Zero-sum game

Discussion (2)

- Scalability
- Frequency of adding new blocks
- Access control

Thank You.