Course:
Introduction to Blockchain:
Technologies, Approaches and Applications

Lecture 2
Blockchain – Technical Details

Sanjay Chaudhary

School of Engineering and Applied Science
Ahmedabad University
Ahmedabad, Gujarat, India

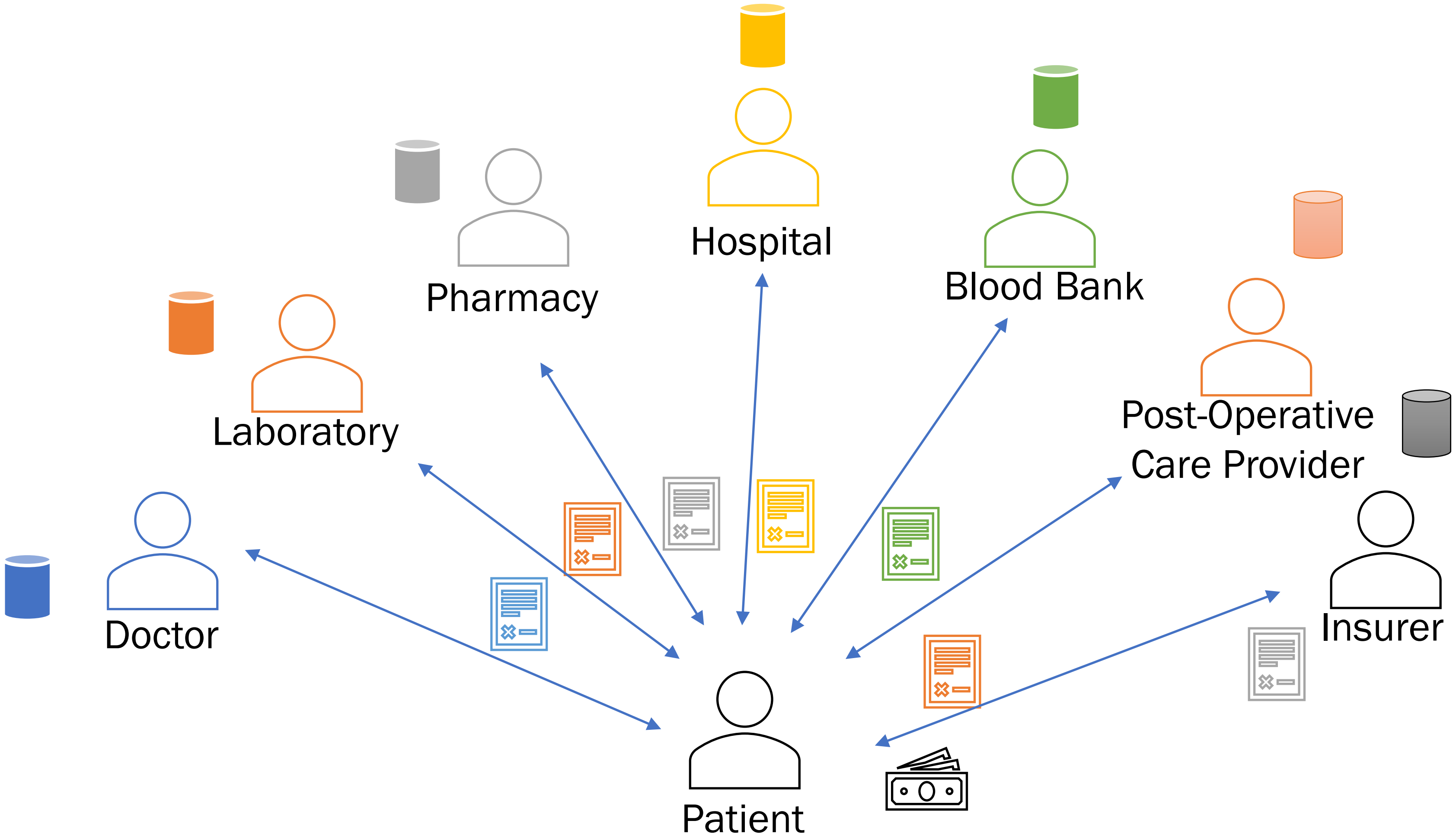
Let’s Test Understanding

Definition

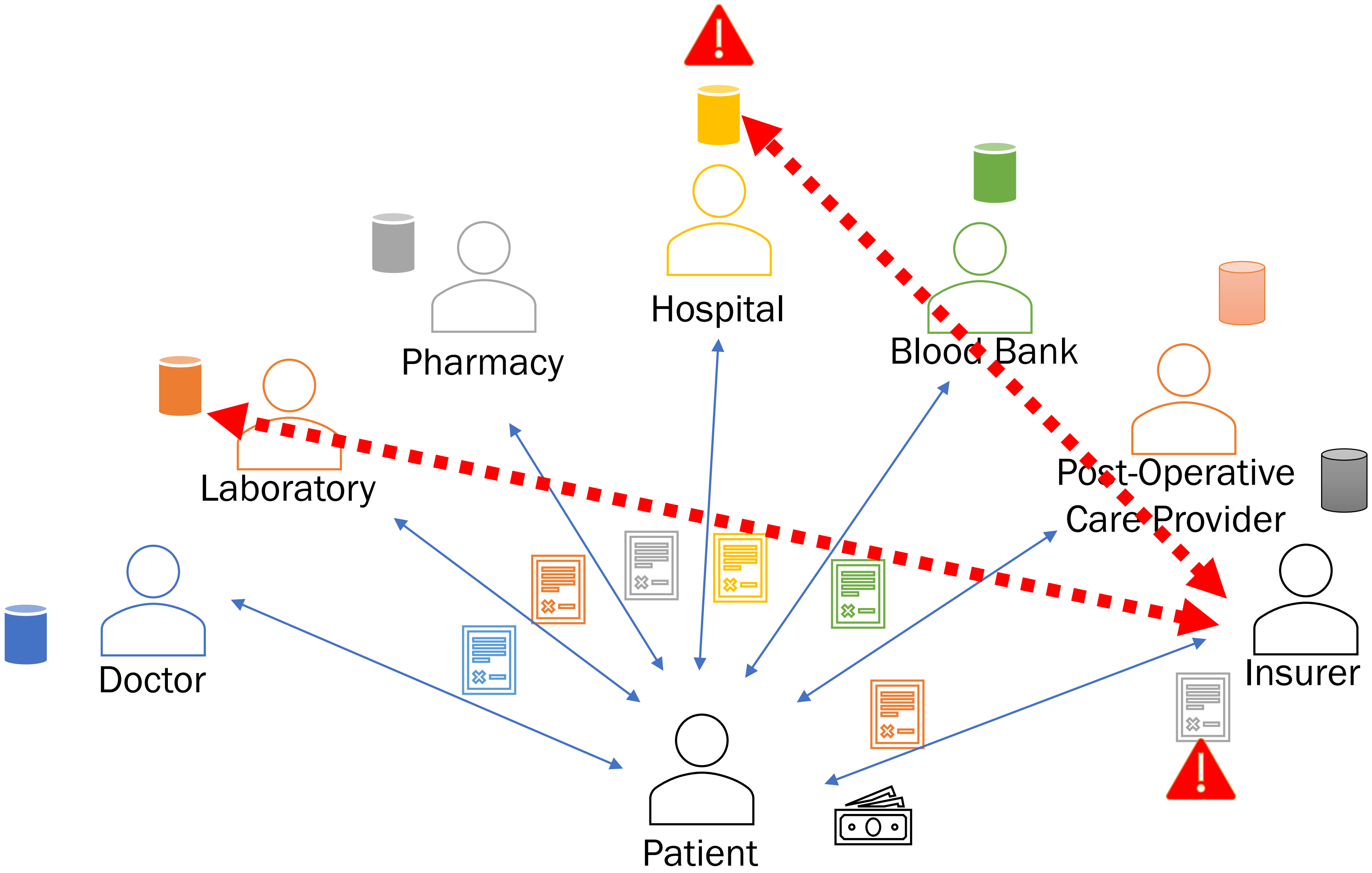
- a digital ledger in which
  - transactions made in bitcoin or another cryptocurrency
  - are recorded chronologically
  - and publicly.

Continuing..

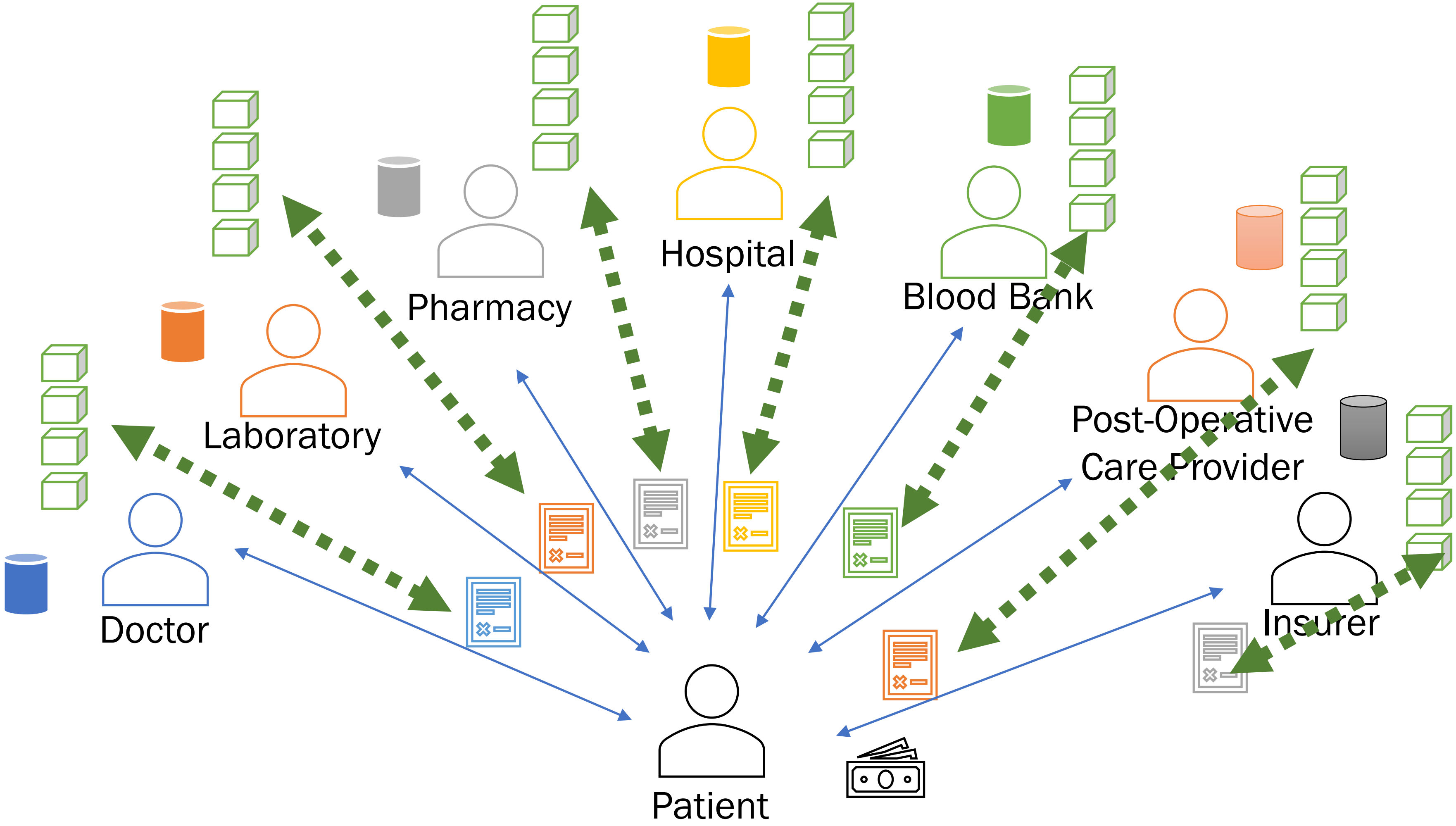
Scenario 2 – Medical Services



Scenario 2 – Medical Services



Scenario 2 – Medical Services



Realizing Desired Capabilities

Realizing Desired Capability - 1

- Engineering Decisions
  - Transaction Information
    - Which details of transactions should be captured?
      - Involved entities
      - Transaction Specification
      - Business process details
      - Time of Transaction
    - How to make sure, only authorized stakeholder can post transaction?
    - How to ascertain validity of the transactions?
    - How to handle continuous stream of transactions?

Realizing Desired Capability - 2

- Engineering Decisions
  - Block
    - Block Structure
      - What information should be included in the block
        - When the block was created?
        - How it is linked to other blocks?
      - How many transactions should be included in one block?
        - Which transactions?
        - How to ensure sequence of transactions?
    - How to the block formation process should be defined
      - How to determine the block is ready to be formed?
      - Who (Which node) will create the block?
      - How to ensure that only one instance block will be accepted?
      - How to ensure block is propagated to remining nodes?

Realizing Desired Capability - 3

- Engineering Decisions
  - Blockchain
    - How to determine, all the nodes has right version of blockchain?
    - How to handle
      - Failures
      - Attacks
      - Conflicts
      - Change in block structure, or protocol
      - Change in policies/governance

Plausible Solutions

- Strategy for Capturing Information
  - Consistent for multiple
    - types of transactions
    - types of stakeholders
    - types of domains
  - Deterministic - Reproducible
  - Protecting the Information
    - Hiding
    - Tamper-proof
  - Unique (Fingerprint)

Solution

- Cryptographic Hash Function
  - Generates Fixed Length Message Digest
  - Avalanche Effect
  - Fast
  - One-way
  - Deterministic
  - Hiding
  - Collision Free

Hash Function

- A cryptography tool that
  - turns any input into
  - a string of characters
  - that serves as a virtually unforgeable digital fingerprint of the data, called a **hash**.
- The values returned by a hash function are called
  - hash values,
  - hash codes,
  - digests, or simply
  - hashes.

Hash Pointers

- a combination of
  - a regular pointer structure with
  - the hash value of the data fragment it points to

- produces an inbuilt data integrity mechanism
  - location evidence
  - tamper evidence

Summary

- This Lecture
  - Requirements for handling
    - Transactions
    - Blocks
    - Blockchain
  - Introduction to Hash
- Next Lecture
  - Structure of Block
  - Mining
  - Consensus Protocols
  - Additional Technical Details

Additional Reading

- Primer on Blockchain
  - How to assess the relevance of distributed ledger technology to international development
    - By USAID
    - https://www.usaid.gov/digital-development/digital-finance/blockchain-primer