BLOCKCHAINS

ARCHITECTURE, DESIGN AND USE CASES

SANDIP CHAKRABORTY
COMPUTER SCIENCE AND ENGINEERING,
IIT KHARAGPUR

PRAVEEN JAYACHANDRAN
IBM RESEARCH,
INDIA

Course Instructors

Sandip Chakraborty
Department of CSE
IIT Kharagpur

Praveen Jayachandran
IBM Research
India

What We’ll Cover in This Course

- A history of blockchain – how the computation environment gradually evolved
- Blockchain – architecture, design and protocol
- Blockchain consensus protocols
- Security and Privacy aspects of Blockchain
- Various use cases – Finance, Supply Chain, Government
- Hyperledger Fabric – a platform for Blockchain development
- Research aspects

What Is A Blockchain

- A **decentralized** **computation and information sharing platform** that enables **multiple authoritative domains**, who **do not trust** each other, to **cooperate, coordinate** and **collaborate** in a **rational decision making process**

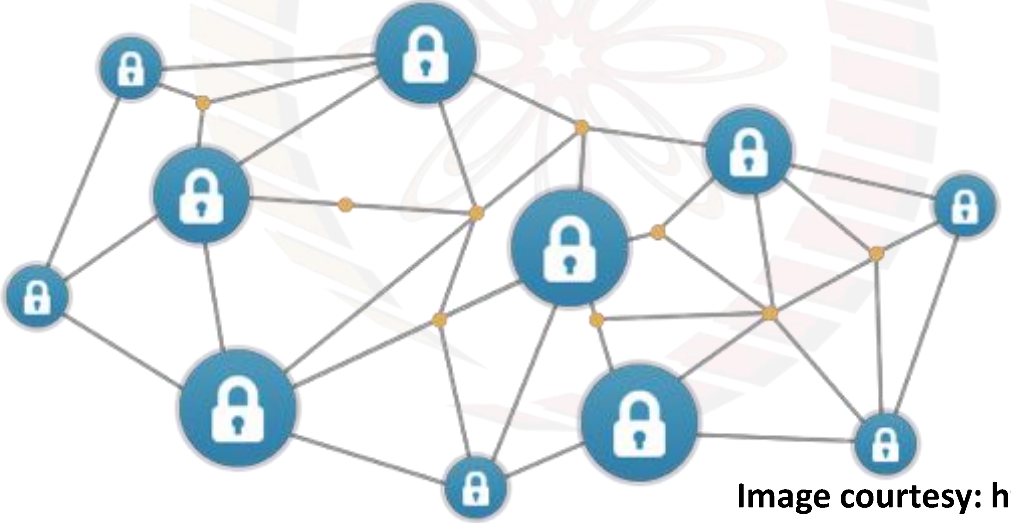
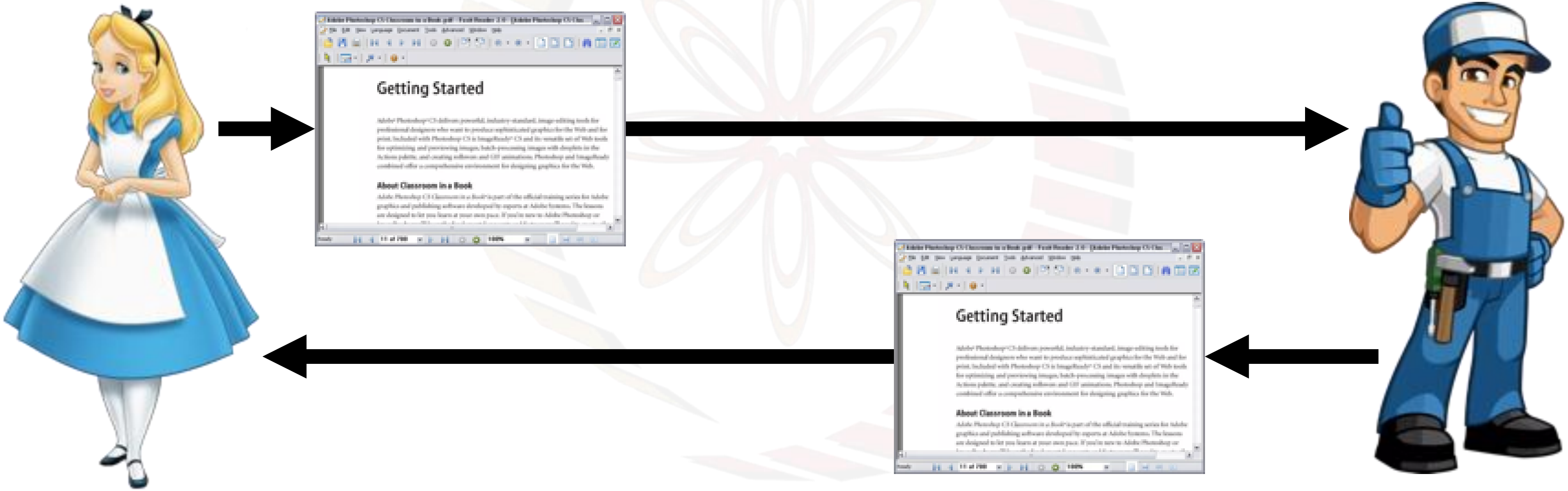


Image courtesy: https://blog.exchangeunion.com

Microsoft Word to Google Doc – Sharing Information

- Traditional way of sharing documents



Getting Started

Adobe Photoshop CS delivers powerful, industry-standard, image-editing tools for professional designers who want to produce sophisticated graphics for the Web and for print. Included with Photoshop CS is ImageReady CS and its versatile set of Web tools for optimizing and previewing images, batch-processing images with droplets in the Actions palette, and creating rollovers and GIF animations. Photoshop and ImageReady combined offer a comprehensive environment for designing graphics for the Web.

About Classroom in a Book

Adobe Photoshop CS Classroom in a Book is part of the official training series for Adobe graphics and publishing software developed by experts at Adobe Systems. The lessons are designed to let you learn at your own pace. If you're new to Adobe Photoshop or

Getting Started

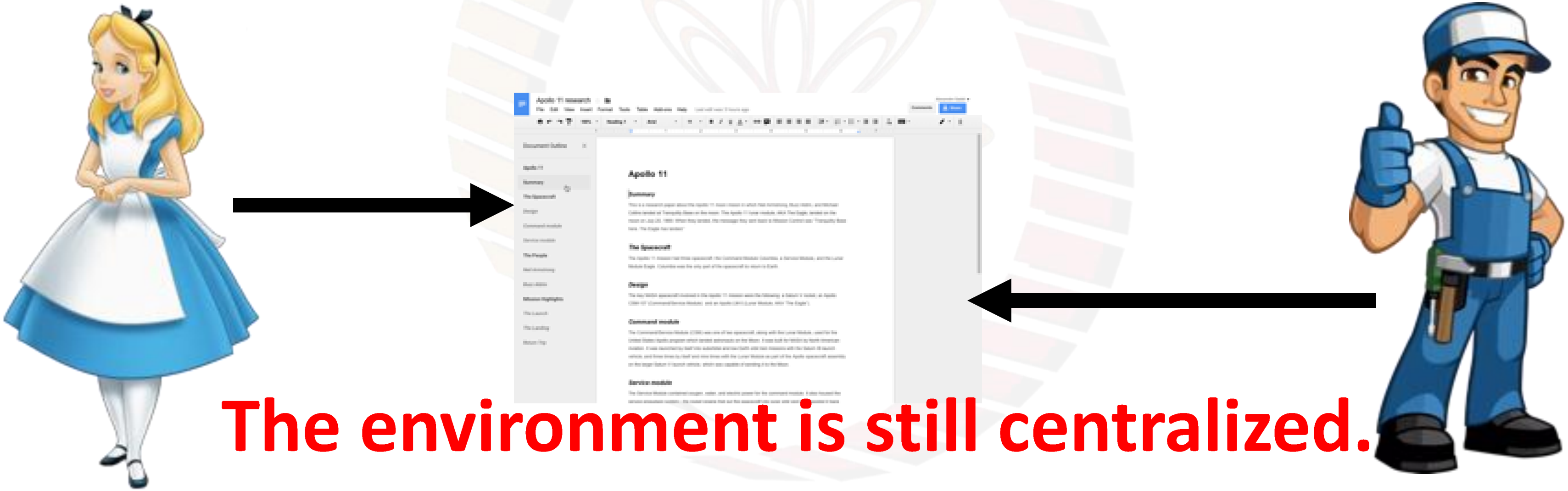
Adobe Photoshop CS delivers powerful, industry-standard, image-editing tools for professional designers who want to produce sophisticated graphics for the Web and for print. Included with Photoshop CS is ImageReady CS and its versatile set of Web tools for optimizing and previewing images, batch-processing images with droplets in the Actions palette, and creating rollovers and GIF animations. Photoshop and ImageReady combined offer a comprehensive environment for designing graphics for the Web.

About Classroom in a Book

Adobe Photoshop CS Classroom in a Book is part of the official training series for Adobe graphics and publishing software developed by experts at Adobe Systems. The lessons are designed to let you learn at your own pace. If you're new to Adobe Photoshop or

Microsoft Word to Google Doc – Sharing Information

- Shared Google doc – both the users can edit simultaneously



Apollo 11 research

File Edit View Insert Format Tools Table Add-ons Help

Document Outline

Apollo 11

Summary

The Spacecraft

Design

Command module

Service module

The People

Neil Armstrong

Buzz Aldrin

Mission Highlights

The Launch

The Landing

Return Trip

Apollo 11

Summary

[illegible]

The Spacecraft

[illegible]

Design

[illegible]

Command module

[illegible]

Service module

[illegible]

The environment is still centralized.

Does centralized system harm?

Problems with a Centralized System

- **A single point of failure**
  - If you do not have sufficient bandwidth to load Google doc, you'll not be able to edit
  - What if the server crashes?

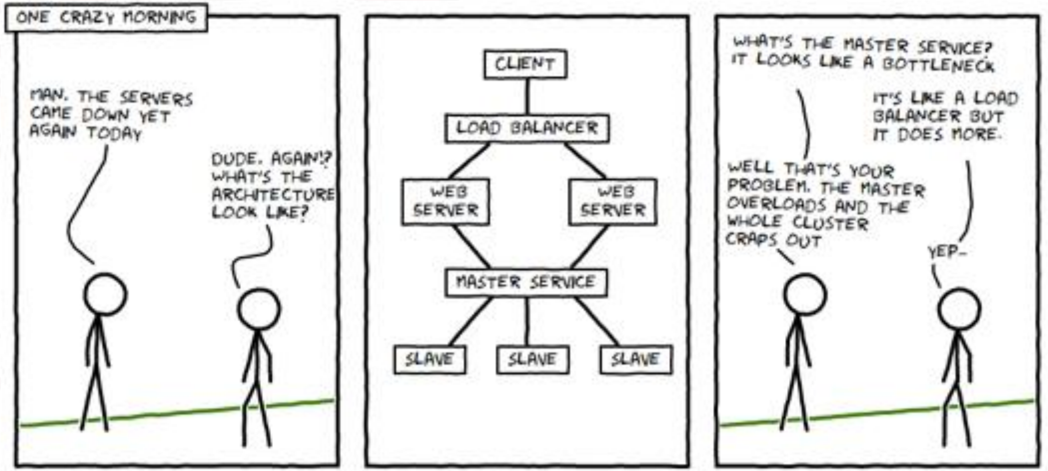
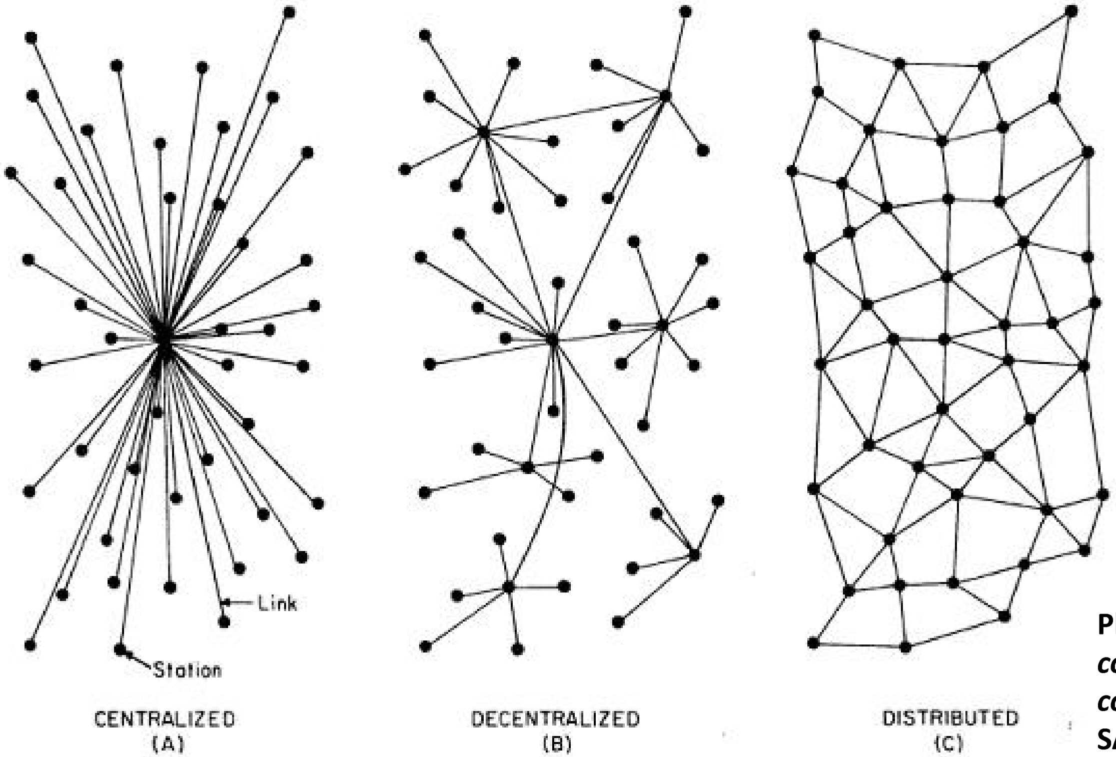

ONE CRAZY MORNING
MAN. THE SERVERS CAME DOWN YET AGAIN TODAY
DUDE. AGAIN!? WHAT'S THE ARCHITECTURE LOOK LIKE?
CLIENT
LOAD BALANCER
WEB SERVER
WEB SERVER
MASTER SERVICE
SLAVE
SLAVE
SLAVE
WHAT'S THE MASTER SERVICE? IT LOOKS LIKE A BOTTLENECK
IT'S LIKE A LOAD BALANCER BUT IT DOES MORE.
WELL THAT'S YOUR PROBLEM. THE MASTER OVERLOADS AND THE WHOLE CLUSTER CRAPS OUT
YEP.

Image courtesy: http://timkellogg.me/

Centralized vs Decentralized vs Distributed

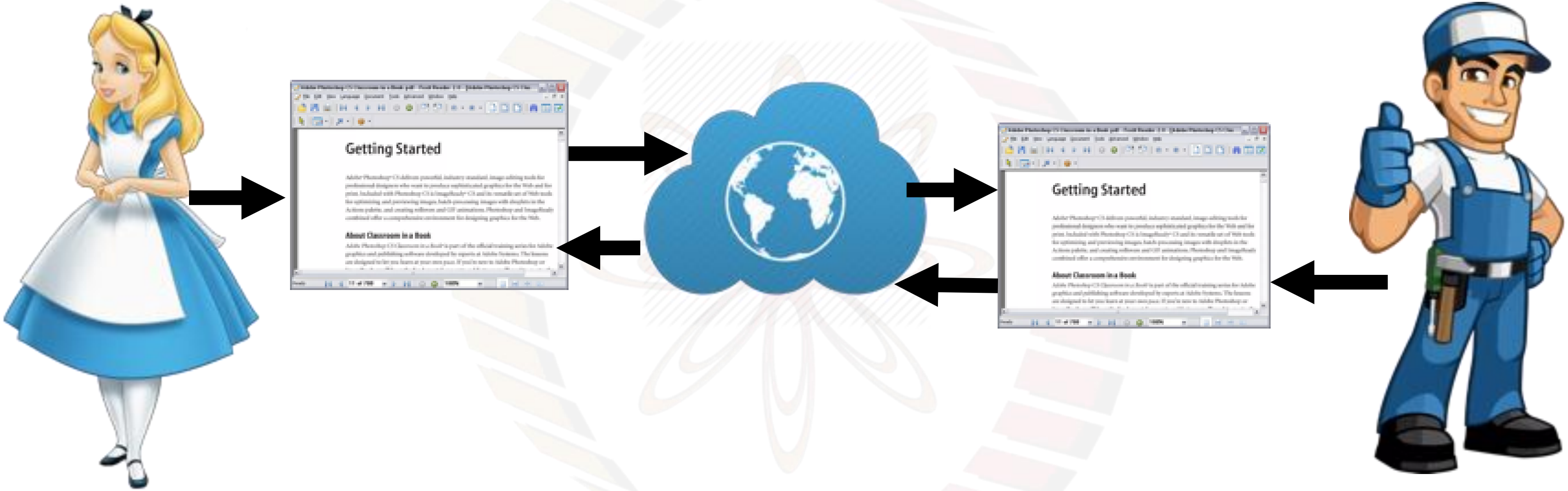


Complete reliance on single point (centralized) is not safe

- **Decentralized**: Multiple points of coordination
- **Distributed**: Everyone collectively execute the job

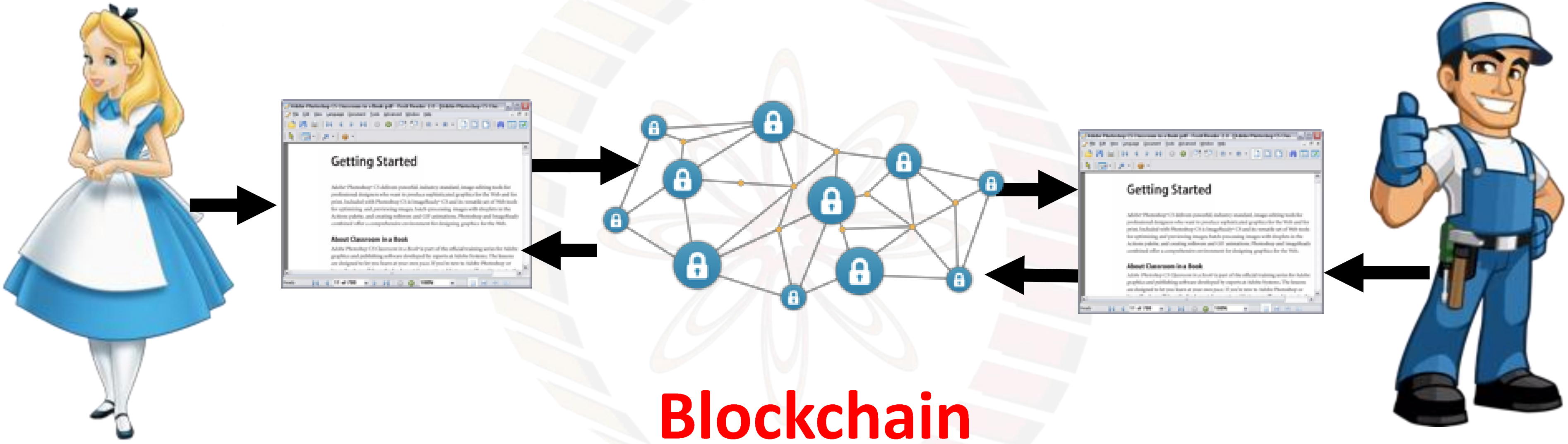
Photo courtesy: Baran, Paul. *On distributed communications: I. Introduction to distributed communications networks*. No. RM3420PR. RAND CORP SANTA MONICA CALIF, 1964.

A Plausibly Ideal Solution



Everyone edits on their local copy of the document – the Internet takes care of ensuring consistency

Blockchain – The Internet Database to Support Decentralization

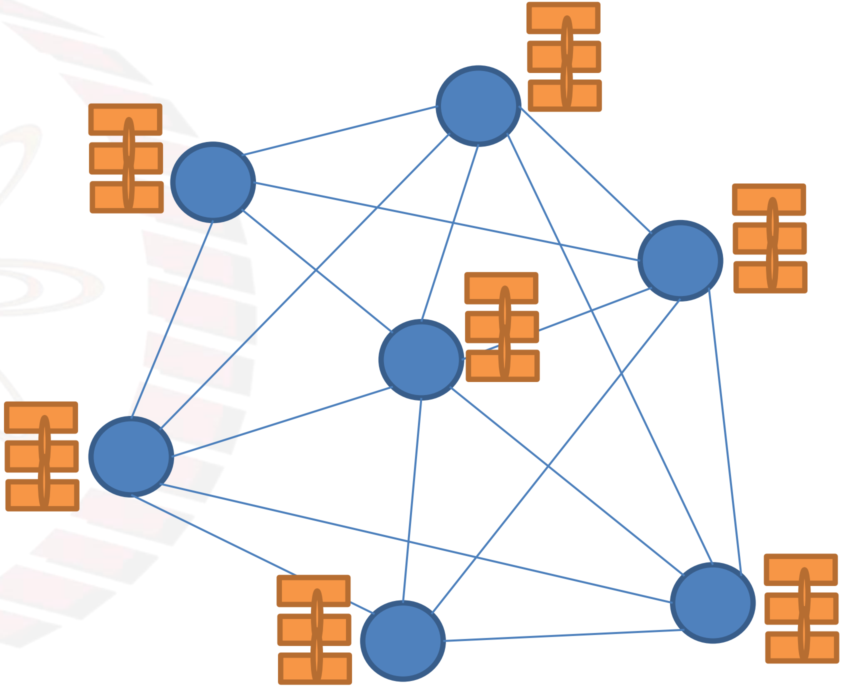


A decentralized database with strong consistency support

A Very Simplified Look of the Blockchain

- Every node maintains **a local copy** of **the global data-sheet**

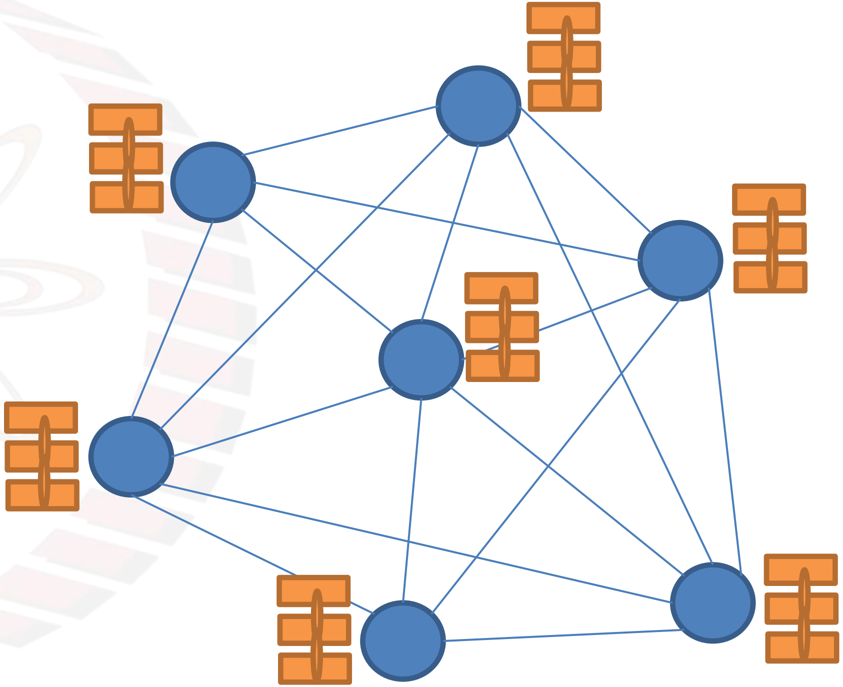
- The system ensures consistency among the local copies
  - *The local copies at every node is identical*
  - *The local copies are always updated based on the global information*



A Very Simplified Look of the Blockchain

- We call this a **Public Ledger**
  - A database of "**historical information**" available to everyone
  - The "**historical information**" may be utilized for future computation

- **An Example:**
  - Say, the historical information are the banking transactions
  - The old transactions are used to validate the new transactions



An Example of Public Ledger from Banking Sectors

Public Ledger of Alice

Alice: ₹100

Alice

₹ 100

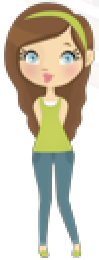
Bob

Alice: ₹100

Public Ledger of Bob

Public Ledger of Eve

Alice: ₹100



Eve

Jane

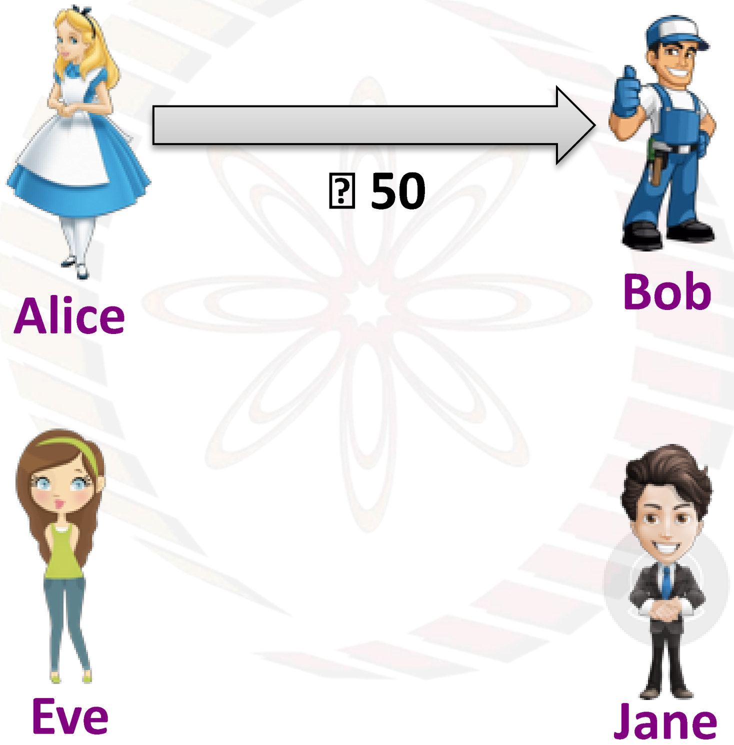
Alice: ₹100

Public Ledger of Jane

An Example of Public Ledger from Banking Sectors

Public Ledger of Alice

Alice: ₹100



Alice: ₹100

Public Ledger of Bob

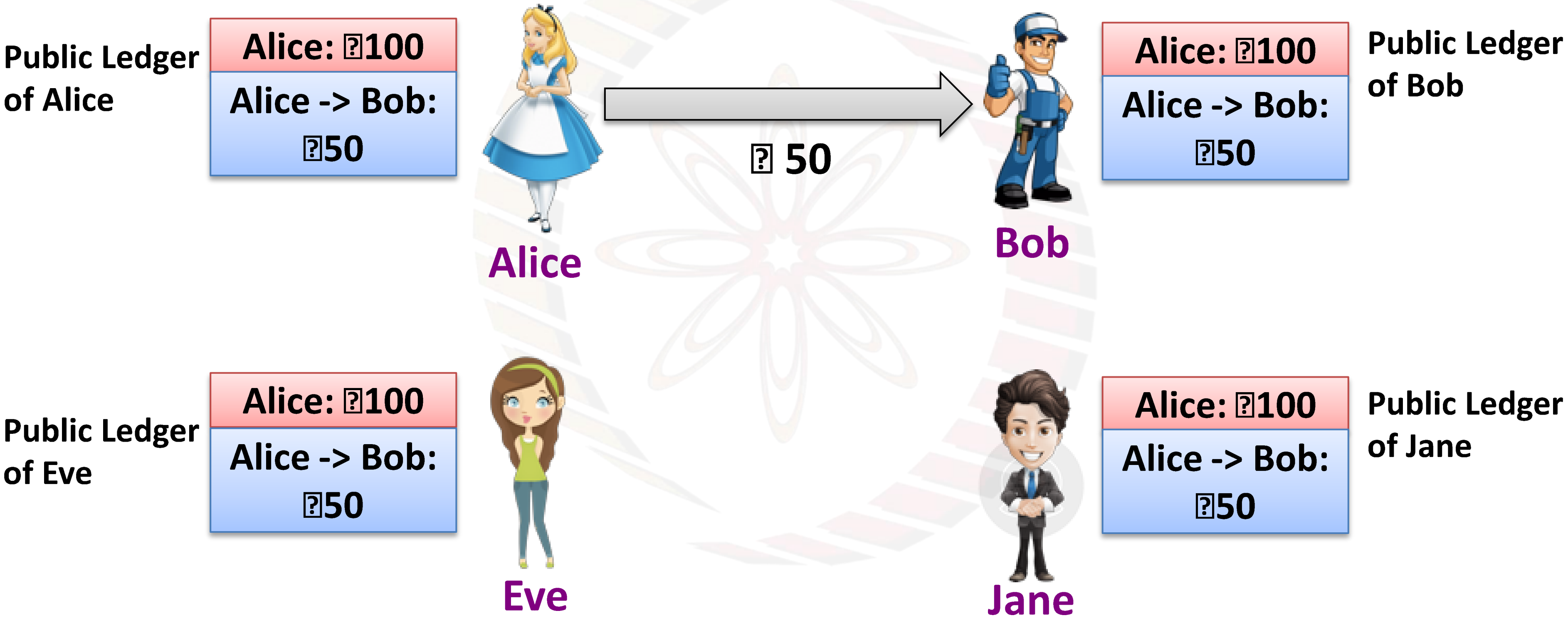
Public Ledger of Eve

Alice: ₹100

Alice: ₹100

Public Ledger of Jane

An Example of Public Ledger from Banking Sectors



Public Ledger of Alice

Alice: 100

Alice -> Bob: 50

Public Ledger of Bob

Alice: 100

Alice -> Bob: 50

Public Ledger of Eve

Alice: 100

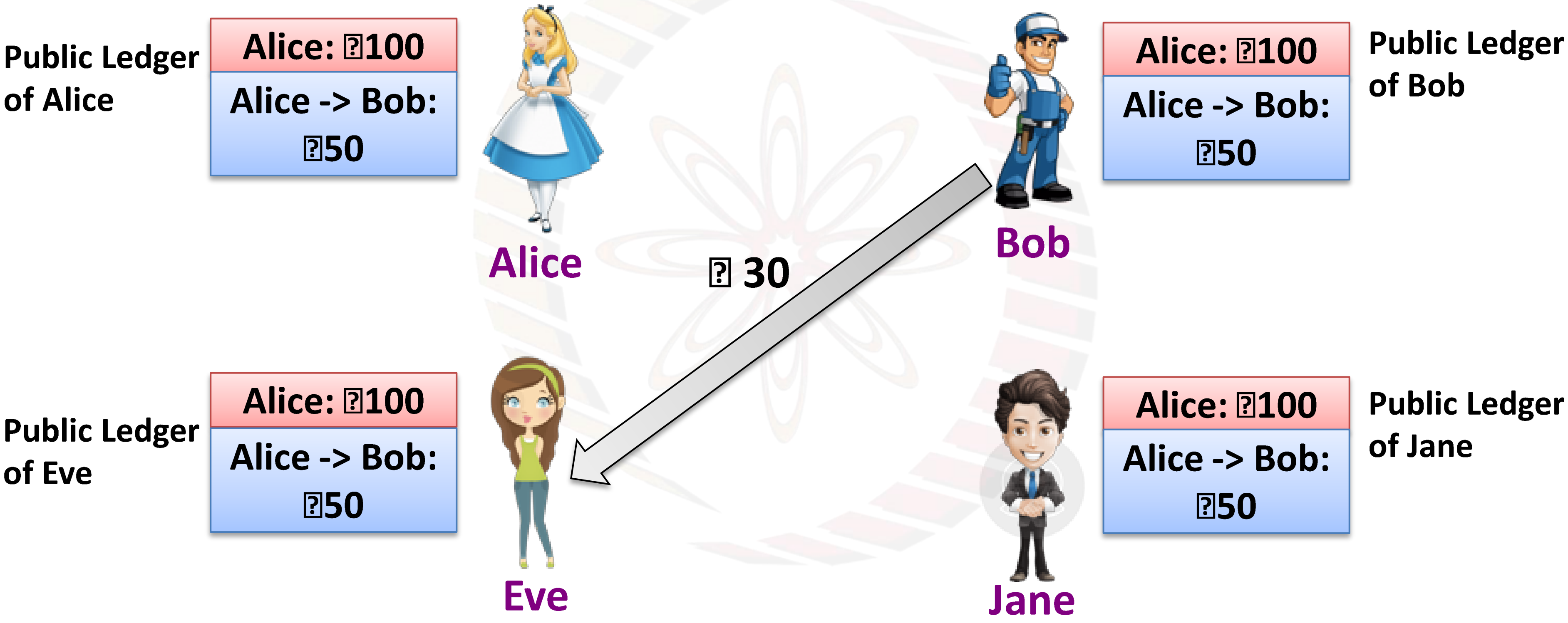
Alice -> Bob: 50

Public Ledger of Jane

Alice: 100

Alice -> Bob: 50

An Example of Public Ledger from Banking Sectors



Public Ledger of Alice

Alice: ⍰100
Alice -> Bob: ⍰50

Public Ledger of Bob

Alice: ⍰100
Alice -> Bob: ⍰50

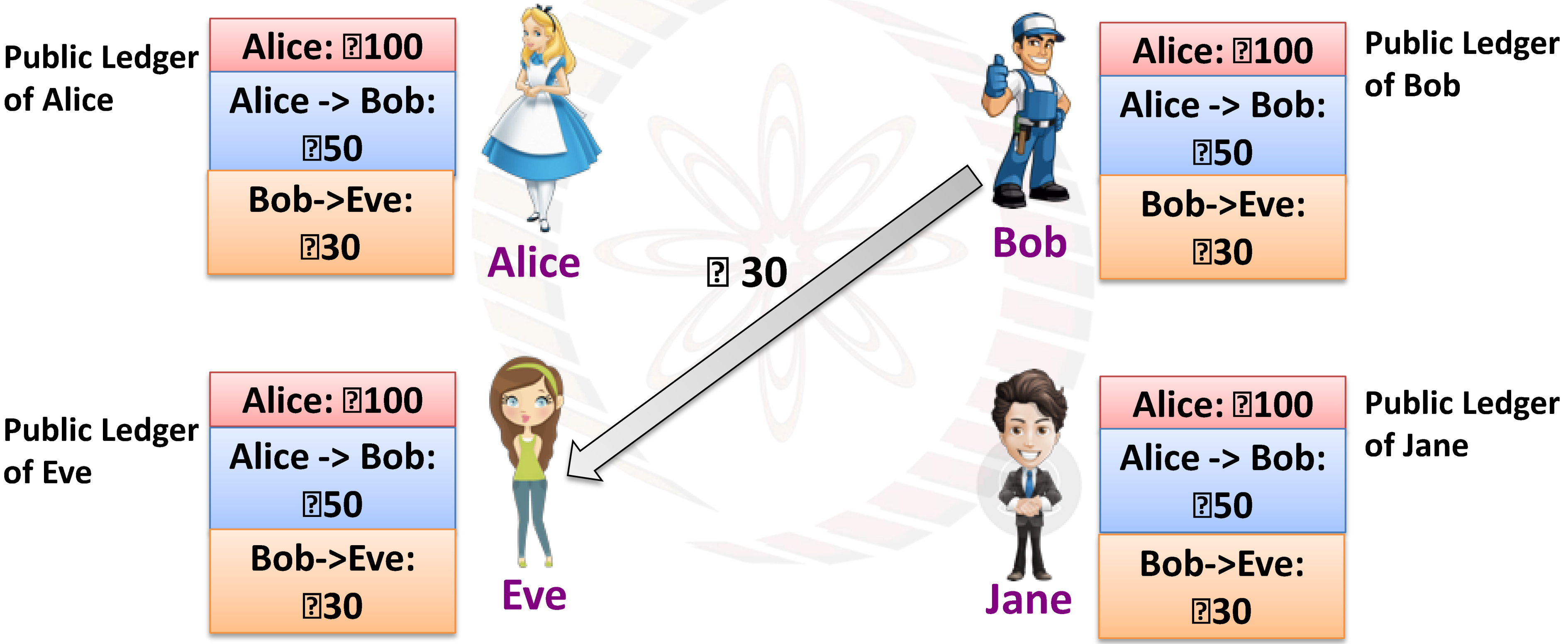
Public Ledger of Eve

Alice: ⍰100
Alice -> Bob: ⍰50

Public Ledger of Jane

Alice: ⍰100
Alice -> Bob: ⍰50

An Example of Public Ledger from Banking Sectors



Public Ledger of Alice

Alice: ⍰100
Alice -> Bob: ⍰50
Bob->Eve: ⍰30

Public Ledger of Bob

Alice: ⍰100
Alice -> Bob: ⍰50
Bob->Eve: ⍰30

Public Ledger of Eve

Alice: ⍰100
Alice -> Bob: ⍰50
Bob->Eve: ⍰30

Public Ledger of Jane

Alice: ⍰100
Alice -> Bob: ⍰50
Bob->Eve: ⍰30

An Example of Public Ledger from Banking Sectors

Public Ledger of Alice

Alice: 100

Alice -> Bob: 50

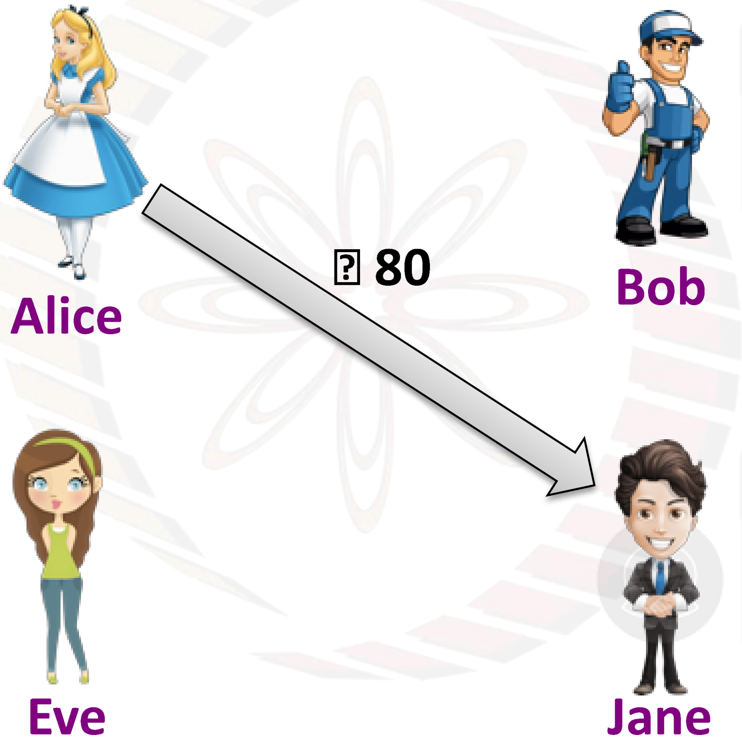
Bob->Eve: 30

Public Ledger of Bob

Alice: 100

Alice -> Bob: 50

Bob->Eve: 30



Public Ledger of Eve

Alice: 100

Alice -> Bob: 50

Bob->Eve: 30

Public Ledger of Jane

Alice: 100

Alice -> Bob: 50

Bob->Eve: 30

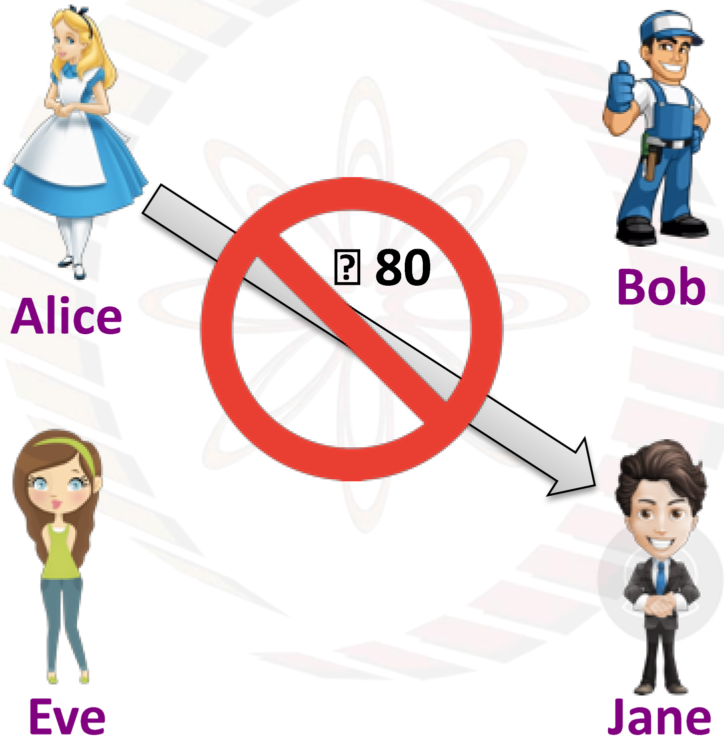
An Example of Public Ledger from Banking Sectors

Public Ledger of Alice

- Alice: ⍰100
- Alice -> Bob: ⍰50
- Bob->Eve: ⍰30

Public Ledger of Bob

- Alice: ⍰100
- Alice -> Bob: ⍰50
- Bob->Eve: ⍰30



Public Ledger of Eve

- Alice: ⍰100
- Alice -> Bob: ⍰50
- Bob->Eve: ⍰30

Public Ledger of Jane

- Alice: ⍰100
- Alice -> Bob: ⍰50
- Bob->Eve: ⍰30

Blockchains and Public Ledgers

- Blockchains work like a public ledger

- However, we need to ensure a number of different aspects
  - **Protocols for Commitment:** Ensure that every *valid transaction* from the clients are committed and included in the blockchain within a finite time.
  - **Consensus**: Ensure that the local copies are consistent and updated.
  - **Security:** The data needs to be *tamper proof*. Note that the clients may act maliciously or can be compromised.
  - **Privacy and Authenticity:** The data (or transactions) belong to various clients; privacy and authenticity needs to be ensured.

Formal Definition of a Blockchain

- A Blockchain is "an open, **distributed ledger** that can record transactions between two parties **efficiently** and in a **verifiable** and **permanent** way" (Iansiti, Lakhani 2017)

- The keywords: **Open** (accessible to all), **Distributed or Decentralized** (no single party control), **efficient (**fast and scalable), **verifiable** (everyone can check the validity of information), **permanent** (the information is persistent)

Iansiti, Marco; Lakhani, Karim R. (January 2017). "The Truth About Blockchain". ***Harvard Business Review*****. Harvard University.**

thank you!