Course:
Introduction to Blockchain:
Technologies, Approaches and Applications

Lecture 1
Introduction to Blockchain

Sanjay Chaudhary

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

Evaluation Plan

- 20% Pop Quiz
- 20% Mid-semester Examination
  - Multiple Choice / Objective and Descriptive Questions
- 20% End-Semester Examination
  - Descriptive Questions
- 40% Project Work
  - Each team having four members
  - Discussions in break up rooms
  - Four rounds of presentations and evaluations

Learning Objectives

- Introduction to Blockchain
  - Need, Key Terms, Technology Landscape
- Underlying Principles
  - Distributed Systems, Cryptography
- Technology Landscape
  - Hyperledger, Ethereum, Multichain, Corda
- Use Cases
  - Government, Industry, Advance Integration
- Advance Topics
  - Governance, Policy, Standards,
- Research Challenges and Opportunities

Course will NOT

- Endorse or promote in any manner
  - × Cryptocurrency mining and trading
- Teach how to
  - × Make money with Bitcoin or other altcoins
  - × Participate in ICOs
  - × Setup mining rigs, exploit hardware
  - × Exploit Vulnerabilities
  - × Participate in trading or selling using cryptocurrencies

Transaction Oriented Systems

Examples, Issues and Challenges

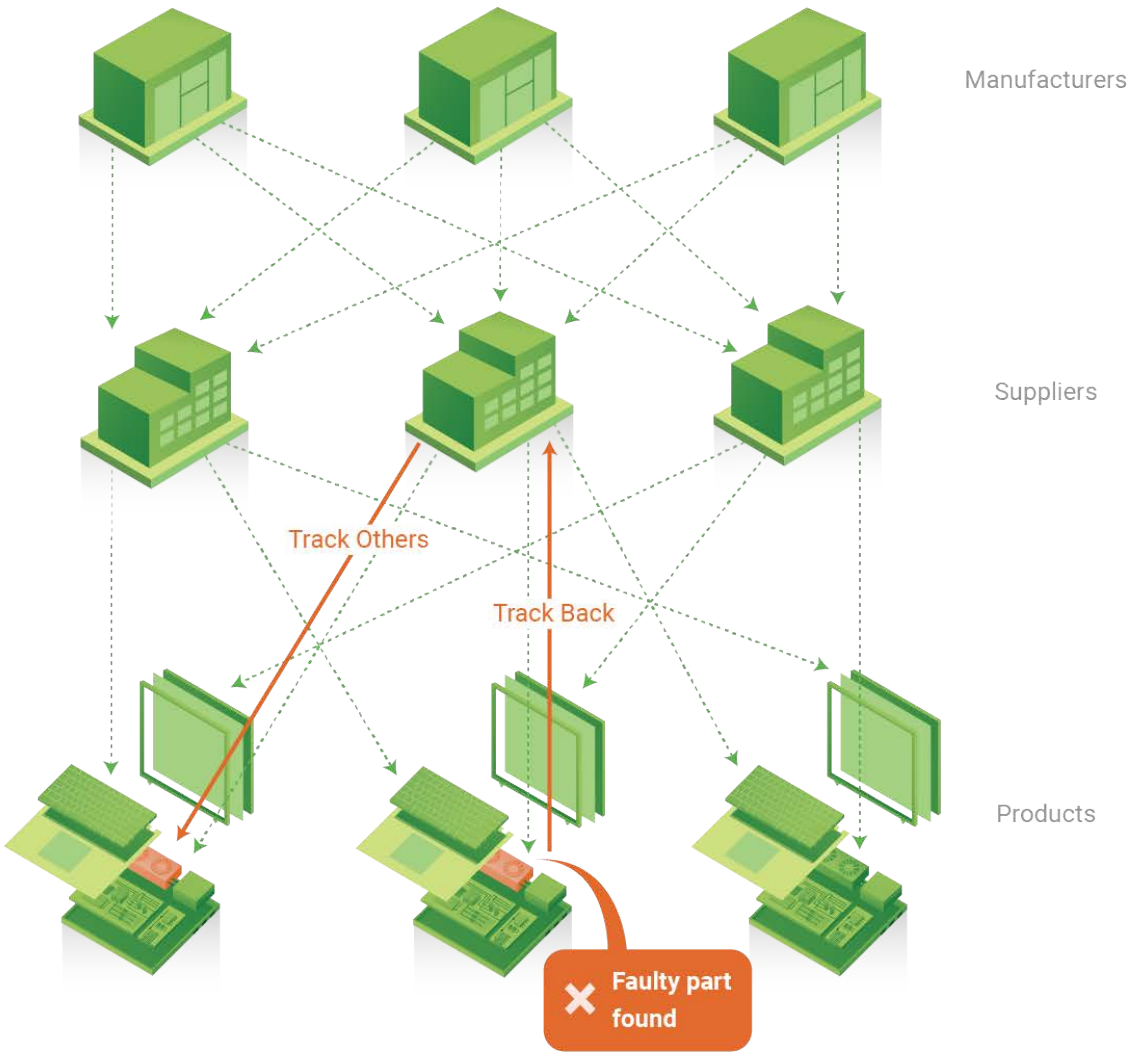
Transaction-Oriented Systems

- Involving end-users
  - Civic Services
    - Identification, Registries, Licensing,..
  - Financial Services
    - Banking, Payments, Remittances,..
  - Health Services
    - Treatment, Labs, Pharmacy, Insurance
  - Asset Management
    - Buy/Sale, Brokerage, Registries, Dispute Resolution..
  - Human Resource Development
    - Education, Training, Recruitment, Background Check,..

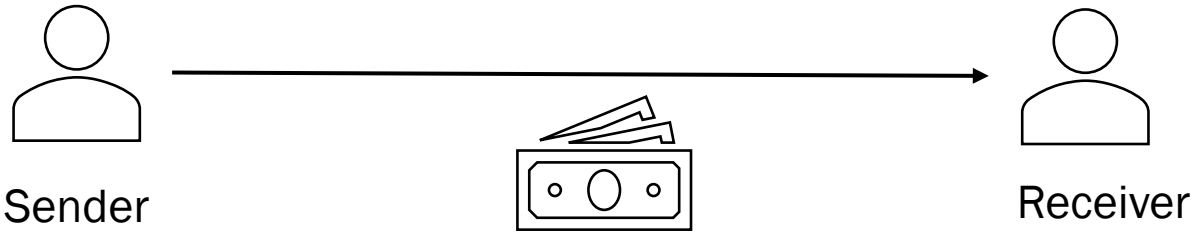
Transaction-Oriented Systems

- Business to Business (B2B),
  - Supply chain
  - Corporate Finance
  - Exchanges and Marketplaces
- Business to Government (B2G)
  - Regulations (Exim, Permits, Licenses,..)
  - Compliance (Audit, Reporting, Standardization,..)
  - Taxation
- Government to Government (G2G)
  - Administration (Identity, Treaties, Cooperation Agreements,.)
  - Cross-border Issues (International Trade,.)

Manufacturing Supply Chain

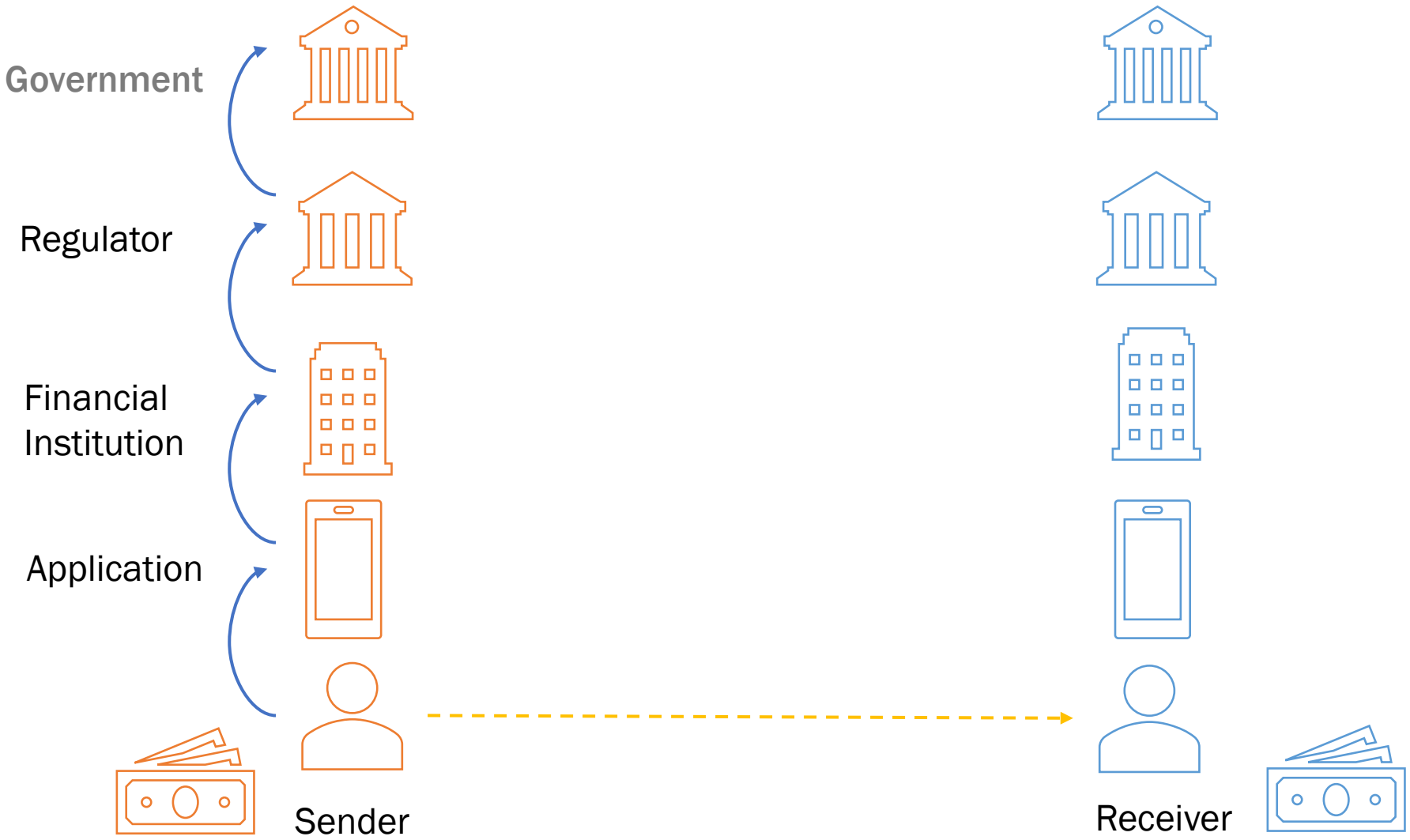


Scenario 1 – Basic Financial Transaction

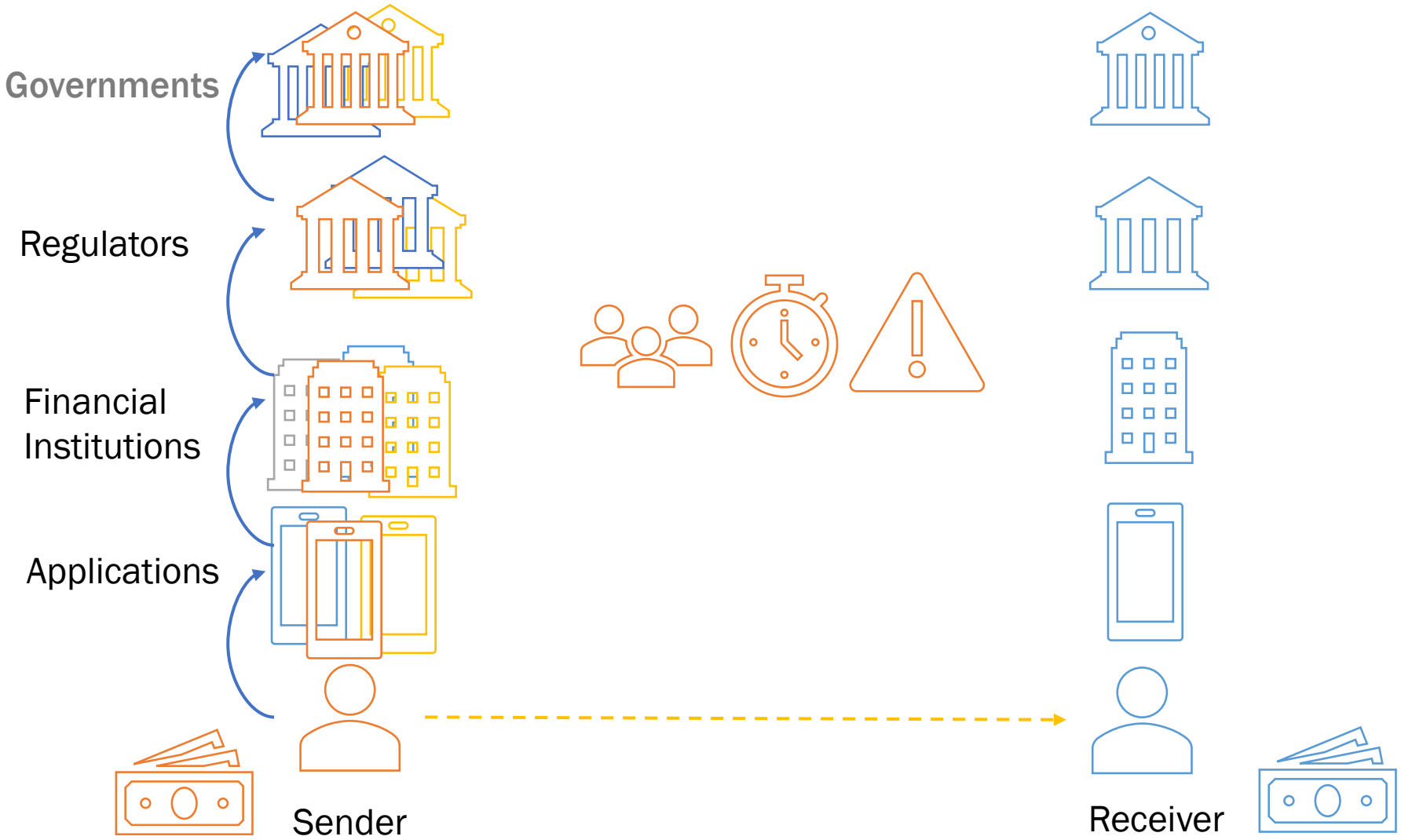


Buyer	Shopping	Seller
Service Consumer	Service	Service Provider
Client	Consultation	Professional
Donor	Donation	Charity

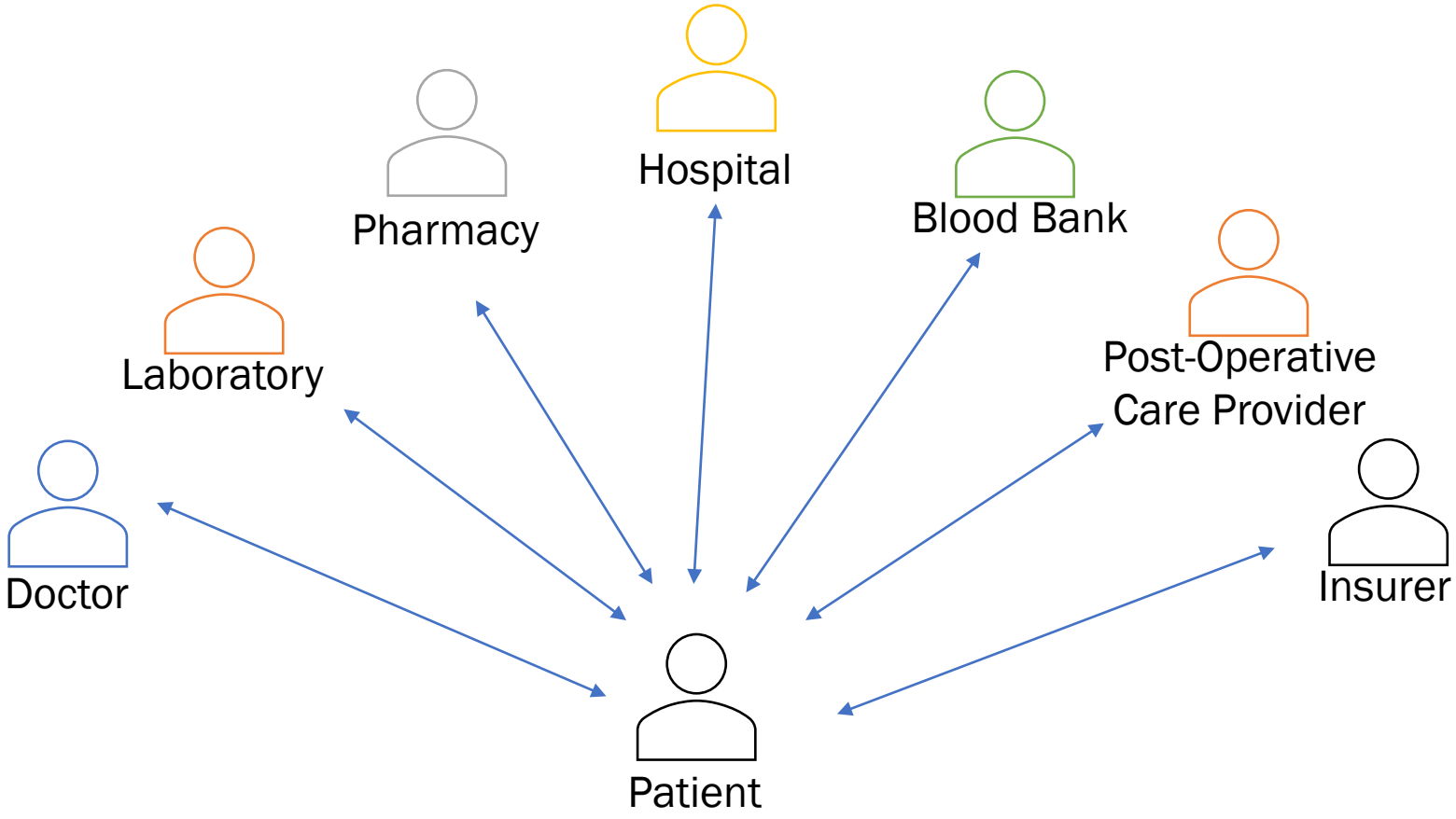
Scenario 1 – Workflow



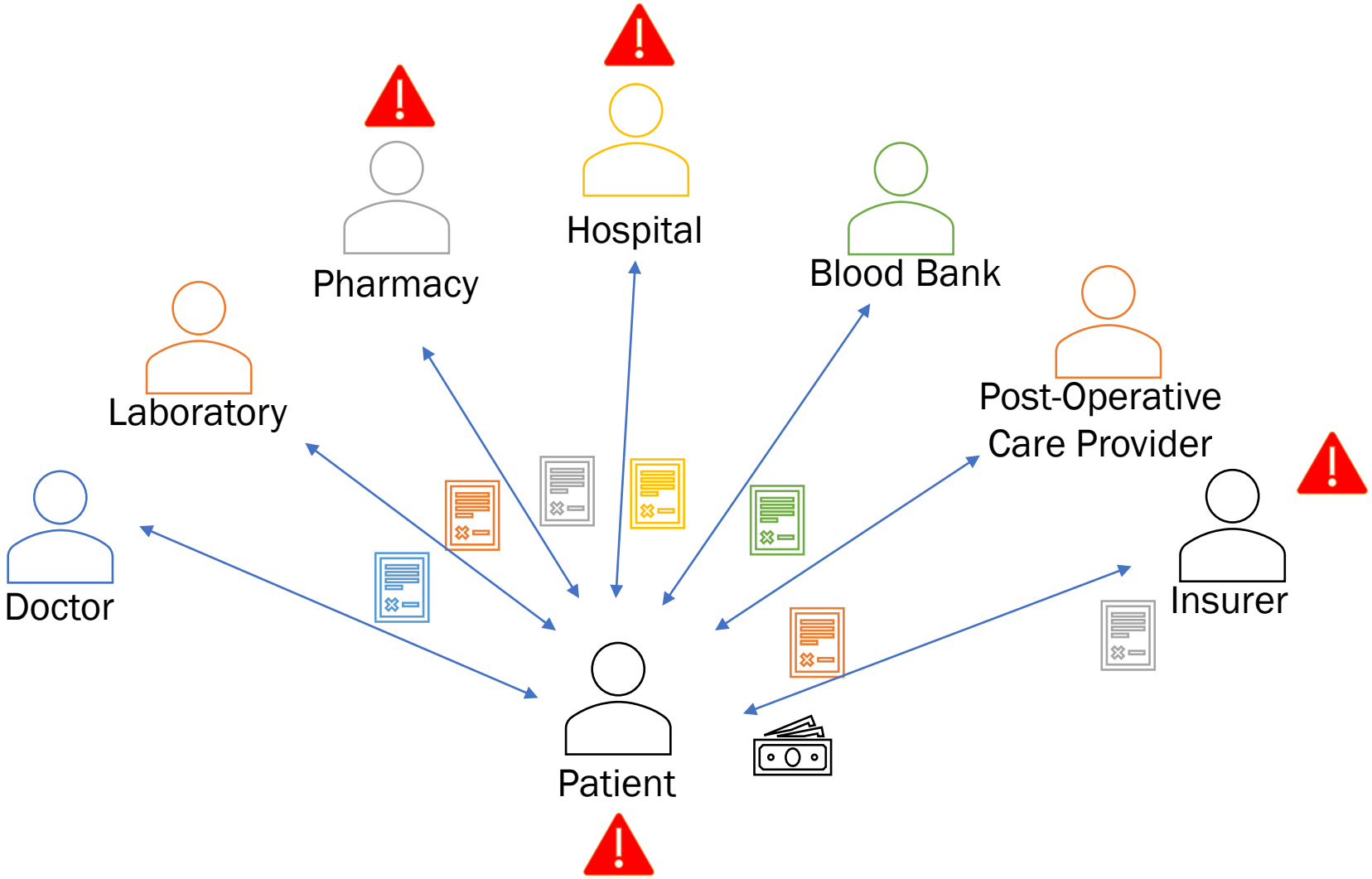
Scenario 1 – Complexities



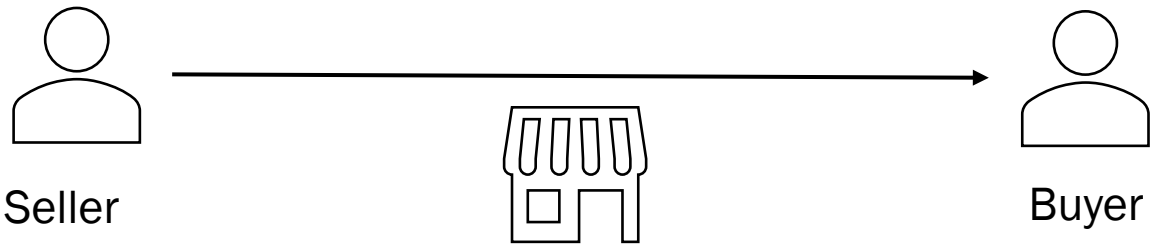
Scenario 2 – Medical Services



Scenario 2 – Medical Services



Scenario 3 – Asset Transfer



Property Owner	Real-Estate	Buyer
Investor	Financial Instrument	Investment Firm
Artist / Creator	Artifact	Art Collector
Rights Owner	Commercial Rights	Commercial Entity

Scenario 3 – Workflow

Listing Broker Lawyer Surveyor Registry Bank

Seller Buyer

Some Observations

- Is there any trust regarding the Stakeholder?
  - Know Your Customer (KYC) Check
  - Background Verification
- Is there any trust regarding validity of Transaction / Claim?
  - Due Diligence
  - Anti Money Laundering (AML) Check
- Is there any trust regarding documents furnished?
  - Validity of Documents

Transaction-Oriented Systems

- Participating Stakeholders
  - Specific Roles, Interests, Intentions and Objectives
  - Complex Requirements and Workflows
  - Dependencies and Touch-points
  - Heterogeneous System Implementations
  - Regulatory and Compliance Requirements
  - Risk Perception and Aversion Capabilities
  - Unique Time and Cost Sensitivity

Results of these Complexities

- Increased
  - Operational Overhead
    - Due Diligence
      - Verify correctness of entity, nature of claims etc.
  - Delays
    - Additional time taken at each intermediate step
  - Costs
    - Additional cost involved at each intermediate step
  - Fraudulent Activities
    - Forgery of Documents, Identity Theft, False Claims,
  - Vulnerabilities
    - Security, Business Continuity
  - Dependencies
    - Relying on third-party service providers, Intermediaries

Results of these Complexities

- Decreased
  - Predictability
    - Of Time, Cost and Quality
  - Transparency
    - Due to silos of intermediaries
  - Trust
    - Related to intermediaries
  - Security
    - Due to increased vulnerability

Causes

- Multiple Stakeholders
  - Lacking Trust
- Inconsistent Record Keeping Practices
  - Inconsistent Ownership information in Asset Registry
  - Inconsistent Transaction information
- Inconsistent Stakeholder Verification
  - Inconsistent Identities
  - Different Authentication and Authorization of Participants
- Inaccessible Systems of Records
  - Reliance on Intermediaries
  - Leading to Forgery
- Insecure Systems
  - Prone to Tampering
  - Vulnerable to Attacks

Plausible Solution

- Consortium of Non-Trusting Participating Stakeholders
  - No Single Controlling Entity
  - Governance Model
- Verifiability of Transaction and Ownerships
  - Agreement on what will be Captured
  - All Can Participate in Validating and Verifying
- Secure Access to Single Version of Truth
  - All Participants have Copy of Record
  - Single/Group of Adversaries can not tamper

Blockchain

Definition and Key Concepts

Blockchain Definition

- A Blockchain allows
  - untrusting parties with common interests to
  - co-create a
  - permanent,
  - unchangeable and
  - transparent
  - record of exchange and
  - processing without relying on
  - a central authority.

- Catherine Mulligan

Blockchain Definition - 2

- (Blockchain is a..)
  - Shared,
  - trusted,
  - public ledger of transactions,
  - that everyone can inspect
  - but which no single user controls.
- It is a
  - cryptographed,
  - secure,
  - tamper-resistant
  - distributed database.

- Blockchain Hub

Blockchain Definition - 3

- A structure for
  - storing data in which
  - groups of valid transactions, called blocks,
  - form a chronological chain,
  - with each block cryptographically linked to the previous one.

- MIT Technology Review

Blockchain Explained

- A blockchain is a decentralized, distributed and public digital ledger that is used to record transactions across many computers so that the record cannot be altered retroactively
- This allows the participants to verify and audit transactions inexpensively.
- A blockchain database is managed autonomously using a peer-to-peer network and a distributed timestamping server.
- They are authenticated by mass collaboration powered by collective self-interests.

- Wikipedia.

Blockchain Explained

- A blockchain is an
  - expanding list of cryptographically signed, irrevocable
  - transactional records
  - shared by all participants in a network.
- Each record contains a
  - time stamp and
  - reference links to previous transactions.
- With this information, anyone with access rights can trace back a transactional event, at any point in its history, belonging to any participant.
- A blockchain is one architectural design of the broader concept of distributed ledgers.

- Gartner, Inc.

Key Components

Key Requirements

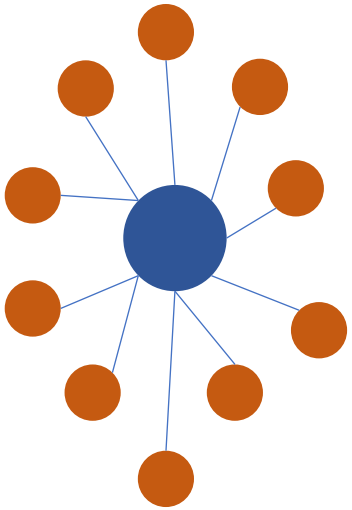
- Shared Ledger
  - Capture Transactions
    - Chronological Manner
      - Time-Stamped
      - Ordered
  - Updated Near-Real-Time
    - Multiple Stakeholders should be able to Append
  - Only Valid Transactions Should be Included
    - Verify Transaction
  - Copy Shared Across Peers
    - All peers must have single shared version on ledger
  - Tamperproof
    - Should not be immutable, permanent, secure record

Distributed Ledger

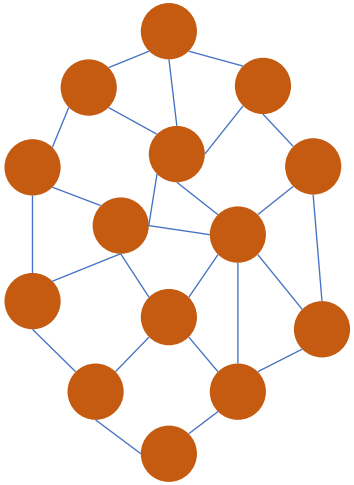
- A *distributed ledger* is a
  - type of database that is shared, replicated, and synchronized
  - among the members of a decentralized network.
- The distributed ledger records the transactions, such as the exchange of assets or data, among the participants in the network.

Decentralization

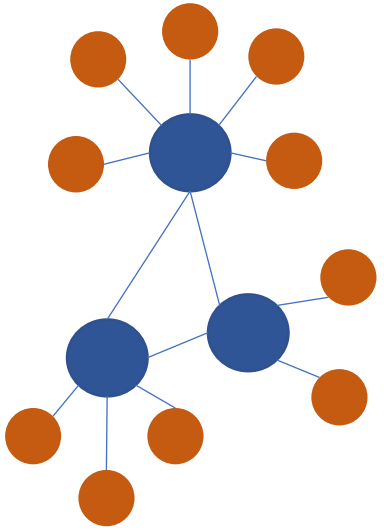
Centralized



Distributed



Decentralized



Decentralization

- A state where there is
  - no central control,
  - power or function, or
  - in reference to infrastructure, no central point of failure.
- Blockchains are
  - politically decentralized (no one controls them) and
  - architecturally decentralized (no infrastructural central point of failure) but they are
  - logically centralized (there is one commonly agreed state and the system behaves like a single computer).

Block

- Blocks are like individual pages of an accounting book. On a Blockchain, a variable number of transactions are recorded per block.

  - Bitcrystals

- A package of data containing multiple transactions over a given period of time

  - Grant Thornton

- A collection of transactions that have happened during a certain amount of time (10 minutes).
- The transactions are bundled in a block and added to the Blockchain.

  - Upfolio

Smart Contract

- A computer program stored in a blockchain that automatically moves digital assets between accounts if conditions encoded in the program are met. It serves as a way to create a mathematically guaranteed promise between two parties.

  - MIT Technology Review

- Computer code that is placed onto a blockchain, and which is set to add certain transactions automatically upon certain trigger events taking place. A smart contract works something like a self-operating escrow account.

  - ICAEW

Wallet

- a file that contains a collection of private keys and communicates with the corresponding blockchain.
- Most commonly found as a web service, mobile app or desktop client, it allows the owners of keys for specific blockchains to
  - trade in the given chain's currencies,
  - initiate blockchain transactions (create, send, trade tokens) and smart contracts

Nodes in Blockchain

- A computer that is participating in a blockchain by posting transactions and maintaining a copy of the ledger.
- Any computer that connects to the blockchain network is called a node.
  - Nodes may enforce the rules of the blockchain
  - Not all nodes are same

Types of Nodes

- Full Node
  - Fully enforces all of the rules of the blockchain
  - Have a record of the entire blockchain
- Light Node
  - Only store a small number of transactions
  - Receives transaction details from full nodes
- Miner Node
  - **Full nodes** that also participate in mining

Consensus

- A process, encoded in software, by which computers in a network, called nodes, reach an agreement about a set of data.

  - MIT Technology Review

- Consensus is achieved when all participants of the network agree on the validity of the transactions, ensuring that the ledgers are exact copies of each other.

  - Block Geeks

- Collective agreement by various computers in a network and allows it to work in a decentralized, P2P manner without the need of central authority to deter dishonest network participants.

  - All Things Crypto

Types of Blockchain

- Public Blockchain
  - anyone in the world can read, anyone in the world can send transactions to and expect to see them included if they are valid, and anyone in the world can participate in the *consensus process* - the process for determining what blocks get added to the chain and what the current state is
- Private Blockchain
  - A private, closed off Blockchain operated within the same company or group for the transfer and sharing of private information but still accountable to strict security protocols.

Types of Blockchain

- Permissioned Blockchains:
  - Permissioned Blockchain networks allow the network to appoint a group of participants in the network who are given the express authority to provide the validation of blocks of transactions. Or, to participate in the consensus mechanism.
- Consortium Blockchains
  - A consortium blockchain is a blockchain where the consensus process is controlled by a pre-selected set of nodes
  - The right to read the blockchain may be public, or restricted to the participants

DAO (Decentralized Autonomous Organization)

- is an organization that is run through rules encoded as computer programs called smart contracts.
- All the transactions and rules of how the DAO functions are recorded and maintained on a Blockchain.
- The concept behind DAOs is the creation of a company that can function without human interaction, therefore removing any bias or fraud risk from its function.

Dapp (Decentralized Application)

- This application and its input and output are like a blockchain transactions, verified and replicated in several nodes of the blockchain.
- A DAPP stores its data on blockchains, and has the same incentivized functions for users with tokens

Characteristics of Blockchain

- Decentralization
- Disintermediation
- Transparency
- Distributed Trust
- Immutability
- Security
- Confidentiality
- Traceability

Determining Suitability of Blockchain

- Are you trying to remove intermediaries or brokers?
- Are you working with digital assets (versus physical assets)?
- Can you create a permanent authoritative record of the digital asset in question?
- Do you require high performance, rapid (~millisecond) transactions?
- Do you intend to store large amounts of non-transactional data as part of your solution?
- Do you want/need to rely on a trusted party? (e.g., for compliance or liability reasons)
- Are you managing contractual relationships or value exchange?
- Do you require shared write access?
- Do contributors know and trust each other?
- Do you need to be able to control functionality?
- Should transactions be public?
- Are contributors interests unified or well-aligned?

Uptake

- National
  - Central Government
    - Niti Aayog
  - State Governments
    - Andhra Pradesh, Kerala, Maharashtra
  - Industry and Consortia
    - Insurers, Automobile, Software,..
- International
  - Government
    - Dubai *(plans to save USD 1.5 B by switching to Blockchain)*, Estonia..
  - Industry Consortia
    - Financial Institutions, Pharmacy, HR, Supply Chain, Real Estate..
  - Universities
    - MIT, Berkeley, Stanford, Oxford, Duke, Cornell, Edinburgh, Delft,..

Things To Do

- Select a transaction-oriented system, and
  - Perform literature search to identify
    - Participating stakeholders
    - Complexities in workflows
    - Vulnerabilities
  - Compare with checklist to determine suitability of Blockchain
  - Propose what type of blockchain will be suitable.

Additional Reading

- Blockchain Beyond the Hype A Practical Framework for Business Leaders
  - White Paper by World Economic Forum
    - https://www.weforum.org/whitepapers/blockchain-beyond-the-hype

Summary

- This Lecture
  - Transaction Oriented Systems
  - Current Challenges
  - Plausible Solutions
  - Blockchain Promise
  - Key Concepts
- Next Lecture
  - Blockchain Building Blocks:
  - Technical Components
  - Consensus Protocol