NPTEL ONLINE CERTIFICATION COURSES

Blockchain and its applications

Prof. Sandip Chakraborty

Department of Computer Science & Engineering
Indian Institute of Technology Kharagpur

Lecture 59: Blockchain for Decentralized Marketplace (Part 1)

CONCEPTS COVERED

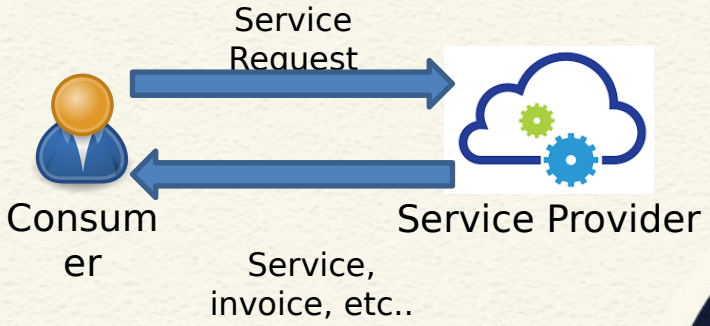
- **Blockchain application for a decentralized marketplace**

KEYWORDS

- Design a blockchain use-case
- Analyzing the requirements

Online Service Providers

- Offers services to the consumers (end-users).
- Use web interface or mobile apps for communicating with consumers.
- Examples:
  - Ecommerce
  - Cloud Service Providers
  - Media Service Providers
  - Logistics Providers

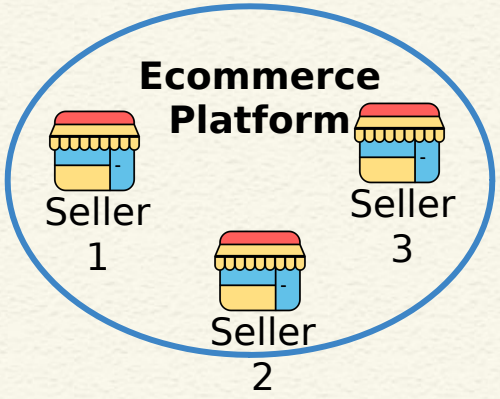


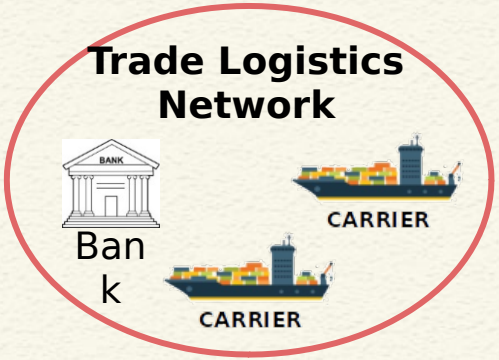
Alibaba.com Azure ebay makemytrip amazon onapp

Online Service Providers

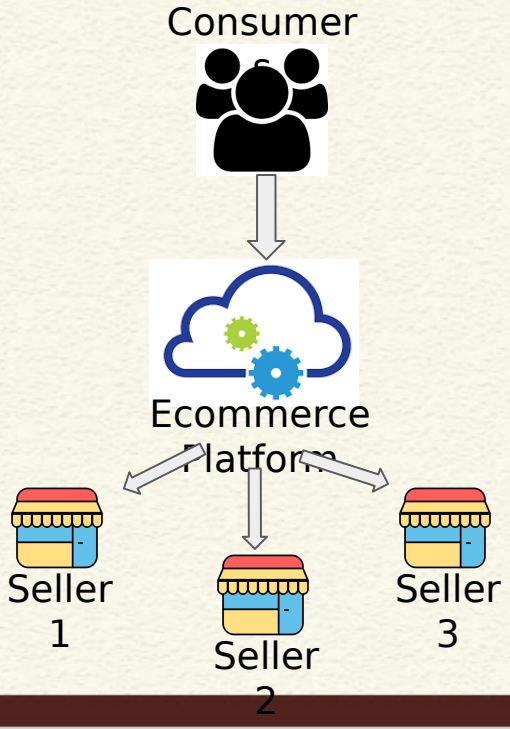
- Multiple service providers (SPs) come into agreement to collaborate.
- Gain access to the common larger set of end-users.
- Offer wider range of services under the same platform.
- Meet user demands by sharing resources.
- Examples:
  - Different sellers under **ebay**, **Amazon**.
  - Cloud infrastructure providers under **OnApp** Federation.
  - Hotels under **trivago**

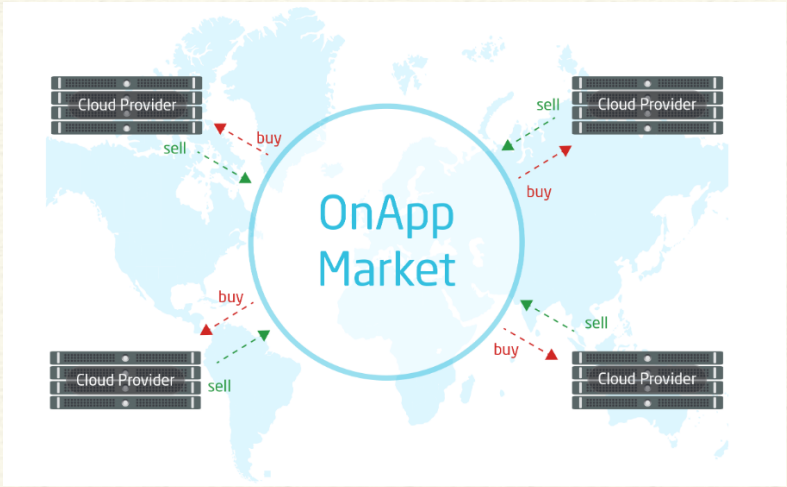
Online Service Providers





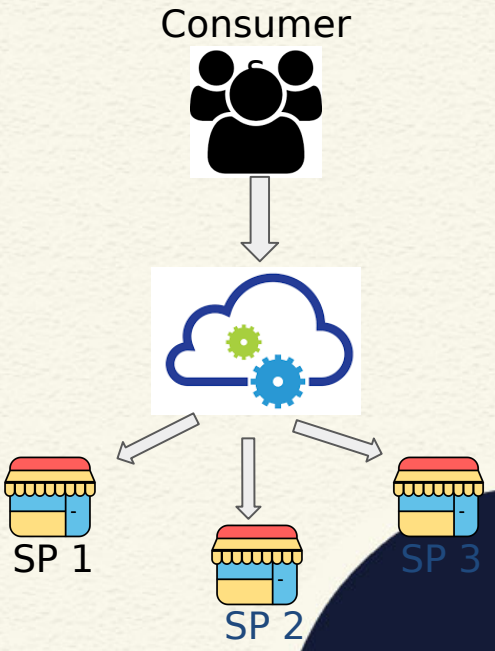
Existing Consortia -- Centralized





Limitations

- Usually governed by a single authority (service broker / marketplace)
  - Unfair business advantage to the broker
- Only service broker or marketplace provider is responsible for communicating with end-users.
- Profit sharing with central broker
- Bias of broker towards a particular provider
- Risk of manipulation & unfair dispute resolution



Objective

- Design a transparent decentralized architecture for service providing consortium, while eliminating any centralized broker/marketplace.

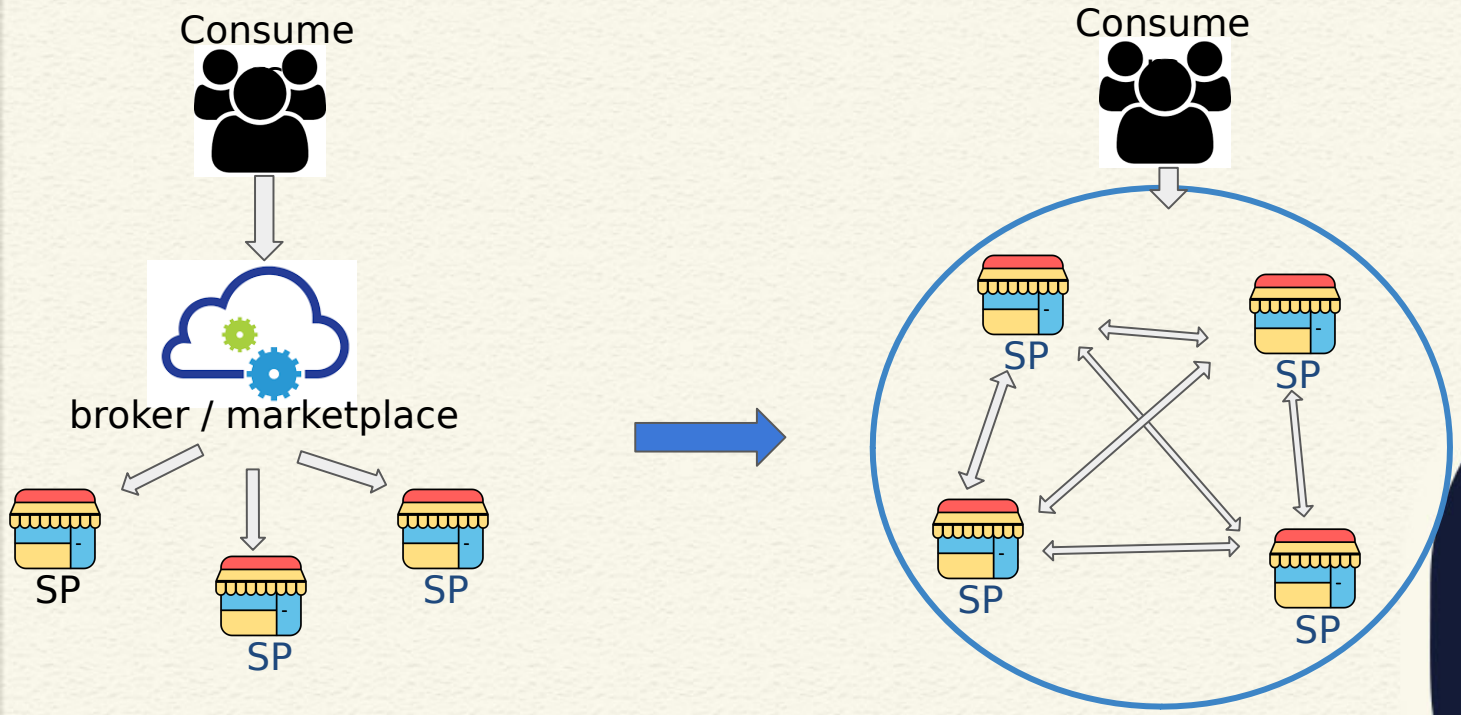
Objective

- Design a transparent decentralized architecture for service providing consortium, while eliminating any centralized broker/marketplace.

Blockchain Interoperability for Service Decentralization, IEEE INFOCOM 2021

Bishakh Chandra Ghosh (IITKGP), Tanay Bhartia (IITKGP), Sourav Kanti Addya (NITK), Sandip Chakraborty (IITKGP)

Centralized to Decentralized



Requirements

- While eliminating the central broker/marketplace, all its functionalities must be preserved in the decentralized consortium architecture:

  - **Unified Interface**
    - The consortium should have a unified interface to its consumers.
    - The interface should be without any centralized broker or agent.
    - Consumers should be able to view catalog, query prices, request for resources, get resource access information and credentials, make payment, etc., through the interface.

Challenges

A. Byzantine behavior of consortium SPs.

- The participating SPs might be byzantine faulty [8].
- SPs can maliciously try to affect the pricing, scheduling, and policies of the consortium.
- SPs can be biased towards certain users and also might try to block certain user requests by affecting the consortium agreement.

B. Byzantine faulty consumers with ability to create multiple identities.

- End-users / consumers can exhibit byzantine fault.
- Each user requests must be agreed upon by the consortium participants to process it correctly.
- Consumers can create as many identities (accounts) as they want introducing the risk of Sybil attacks[8].

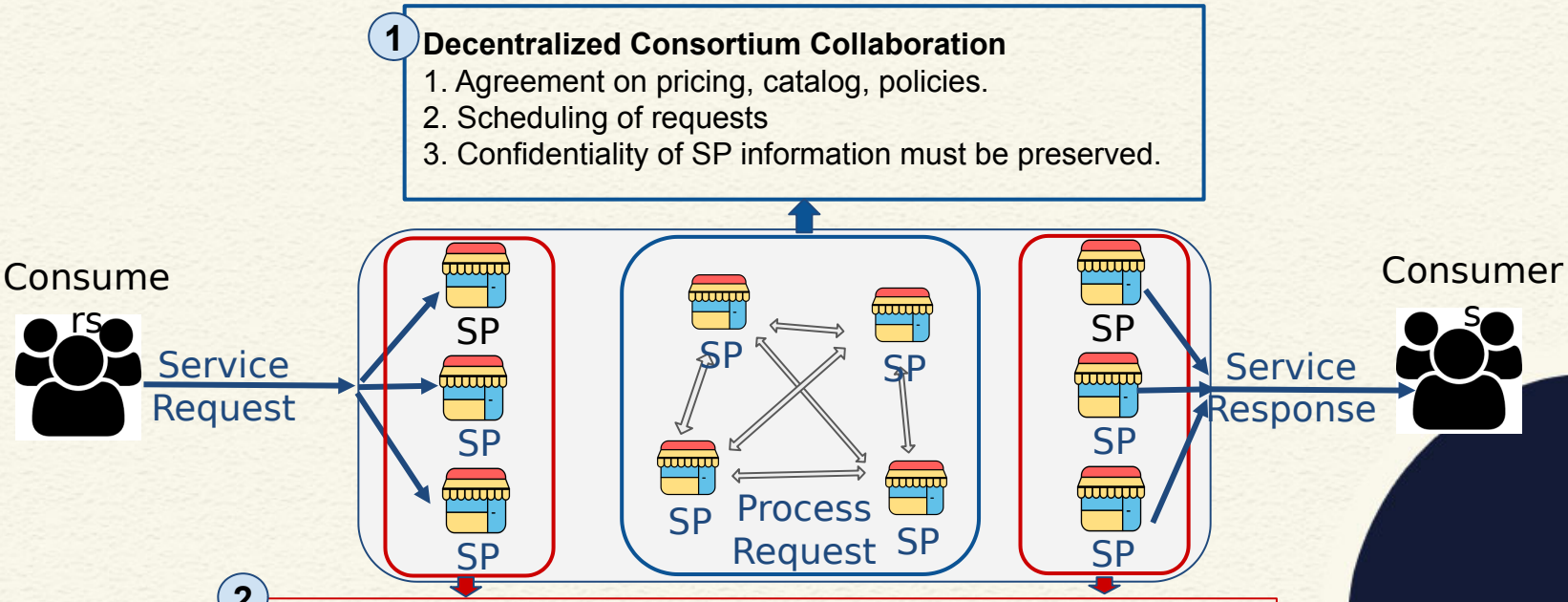
C. Verifiability and confidentiality of information from the consortium

- There is no single trusted spokesperson of the consortium.
- The results of the consortium is based on agreement of the SPs.
- This agreement must be manifested outside the federation, and should be verifiable by the end-users.
- Sensitive consortium response must remain confidential between the consumers and the SPs.

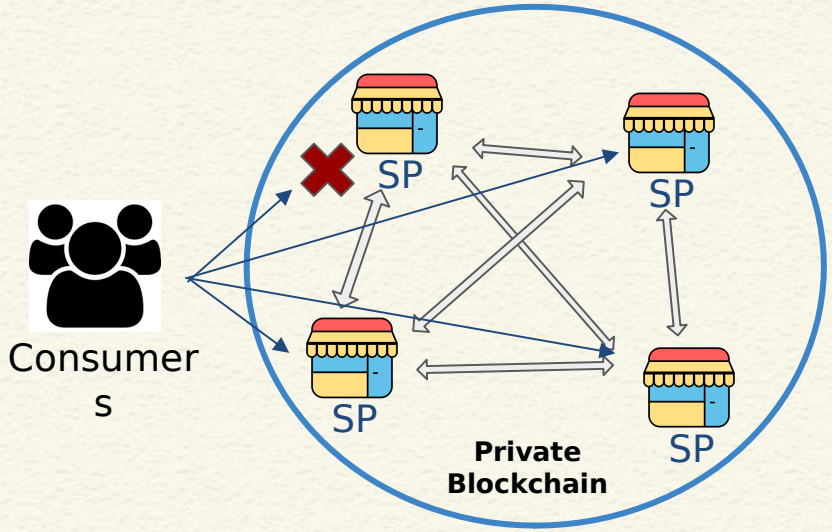
Threat Models

- **Byzantine faults:** We consider that at most 1/3 of the SPs may be Byzantine Faulty. Non-faulty consumers control majority of computing power.
- **Sybil attacks:** End-user consumers can create multiple accounts/identities for accessing the consortium services.
- **Impersonation attacks:** Decentralized consortium does not have a single spokesperson. A malicious SP might try to deceive a consumer by posing as the consortium's spokesperson.
- **Leakage of sensitive information:** Sensitive information of the consortium as well as users might be exposed while passed over the decentralized network.

Architectural Requirements



Decentralized Consortium Interface



Decentralized Consortium Interface

- **How user requests reach the Consortium?**
- No single spokesperson for the consortium.
  - No single web portal or address available for communication.
- Simple solutions like a broadcast from the consumers to the closed network will not work.
  - Messages might be lost
  - Messages might arrive out of order.
- Consumers might be byzantine faulty and try to partition the consortium.

Decentralized Consortium Interface

Required Guarantees:

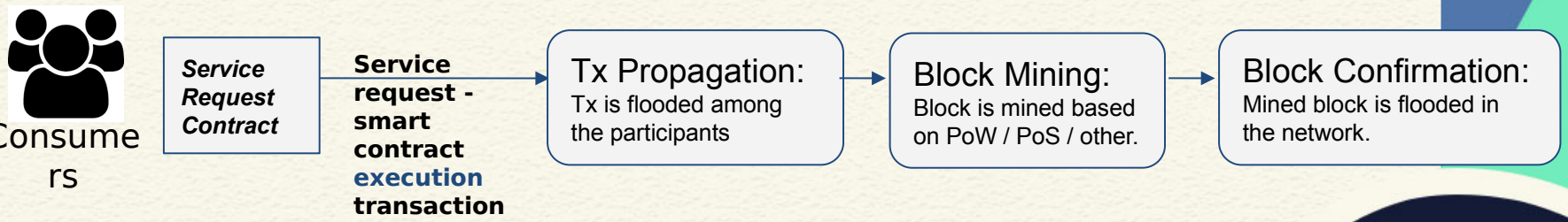
1. **Consortium Interface Safety -** Non faulty SPs receive the same set of consumer requests and in the same order.

2. **Consortium Interface Liveness -** All non faulty consumer requests are eventually received by the consortium.

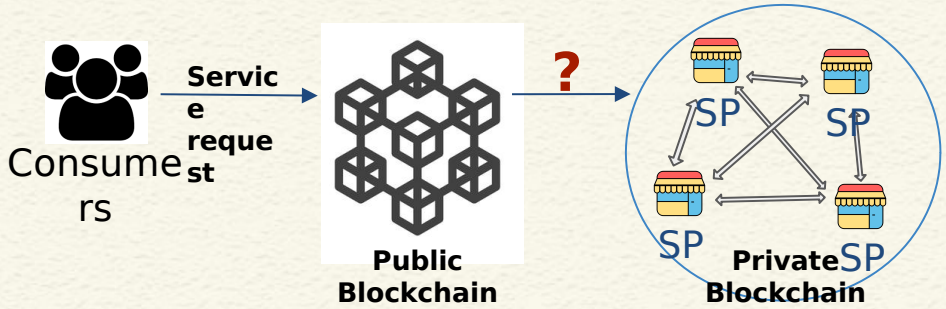
Designing the Interface

- **Use public blockchain for the interface.**
- Any user can join the network and avail services by issuing transactions.
- Smart contract (having a fixed logical address), act as the single point of contact.
- Mining process mines blocks with the transactions.
- The network has **consensus on each block => Consensus on each user request**.
- Each **block has a fixed ordering of transactions => Consensus on order of user requests.**

Designing the Interface



Transferring Consensus to the Consortium

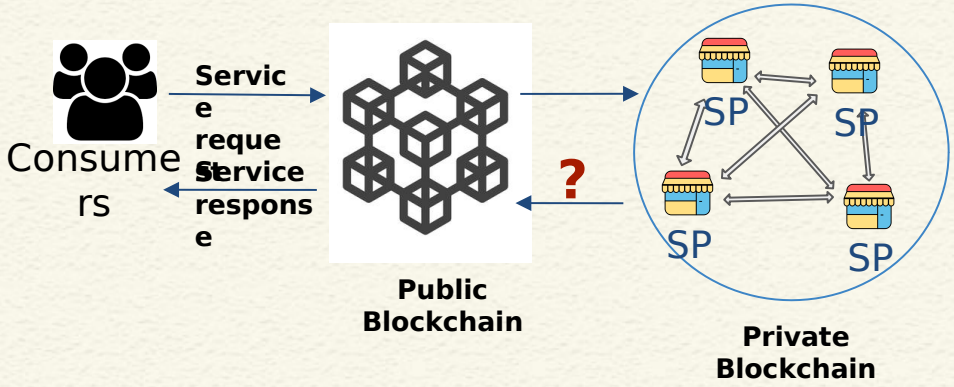


Transferring Consensus to the Consortium

Consortium SPs cannot simply pick requests from the permissionless blockchain and start processing:

1. Some consortium members might not get the mined block in time and thus cannot participate in its scheduling.
2. Malicious consortium members may introduce and schedule invalid consumer requests that are not mined at all.
3. Consensus protocol like PoW, often goes through **temporary forks.** (Network is partitioned into two or more parts with different accepted blocks.)

Transferring Verifiable Response



Transferring Verifiable Response

A single SP cannot simply post a response of the Consortium back to the users.

1. Consortium response is always based on a consensus on the same.
2. **The consortium consensus has no manifestation outside the private blockchain.**
3. **The consortium consensus on response must be verifiable by the end-users.**
4. **Confidentiality** of the response has to be preserved while transferring across the public blockchain network.

Transferring Verifiable Response

A single SP cannot simply post a response of the Consortium back to the users.

How do we solve this problem?

3. **The consortium consensus on response must be verifiable by the end-users.**
4. **Confidentiality** of the response has to be preserved while transferring across the public blockchain network.


Thank
you