NPTEL ONLINE CERTIFICATION COURSES

Blockchain and its applications

Prof. Sandip Chakraborty

Department of Computer Science & Engineering
Indian Institute of Technology Kharagpur

Lecture 56: A Potential Use Case – From a Critics Perspective

CONCEPTS COVERED

- **Land Registry Records – Can we use a Blockchain?**

KEYWORDS

- **Requirement analysis**
- **Tradeoff analysis**

Maintaining Land Registry Records

- Historically, land registries were paper-based
  - Can be lost, destroyed, falsified, or otherwise manipulated
- Selling a property (land)
  - Owner has to prove the ownership
- A complex business network – multiple realtors, inspectors, appraisers, escrow
  - Help people to do the best purchase / sell of the property

Real Estate Scams and Frauds

Home / Cities / Pune News / Beed police arrest addl collector N R Shelke in land scam

PUNE NEWS

Beed police arrest addl collector N R Shelke in land scam

The Beed Police arrested additional collector N R Shelke from Aura... Sunday, in connection with a multi-crore land scam in Chinc... district.

Home / Cities / Lucknow News / Shine City fraud case: Three accused booked under Gangsters ...

LUCKNOW NEWS

Shine City fraud case: Three accused booked under Gangsters Act in Varanasi

Commissioner of police, Varanasi, A Satish Ganesh said real estate and multi-level ...arketing company's chief managing director Rashid Naseem, its managing director ...seem and director Amitabh Shrivastav had been booked under the Gangsters

Seniors often targeted in realty fraud

SBI ex-chairman held for fraud in selling Raj hotel below market price

THE TIMES OF IN...

City Bhubaneswar Mumbai Delhi Bengaluru Hyderabad Kolkata Chennai Agra Agartala Ahmedabad

CRIME CIVIC ISSUES POLITICS SCHOOL AND COLLEGES ODISHA ELECTIONS WEATHER EVENTS

Odisha high court's payoff rider for govt on Cuttack land

Jatmohan patnaik / TNN / Oct 29, 2021, 12:22 IST

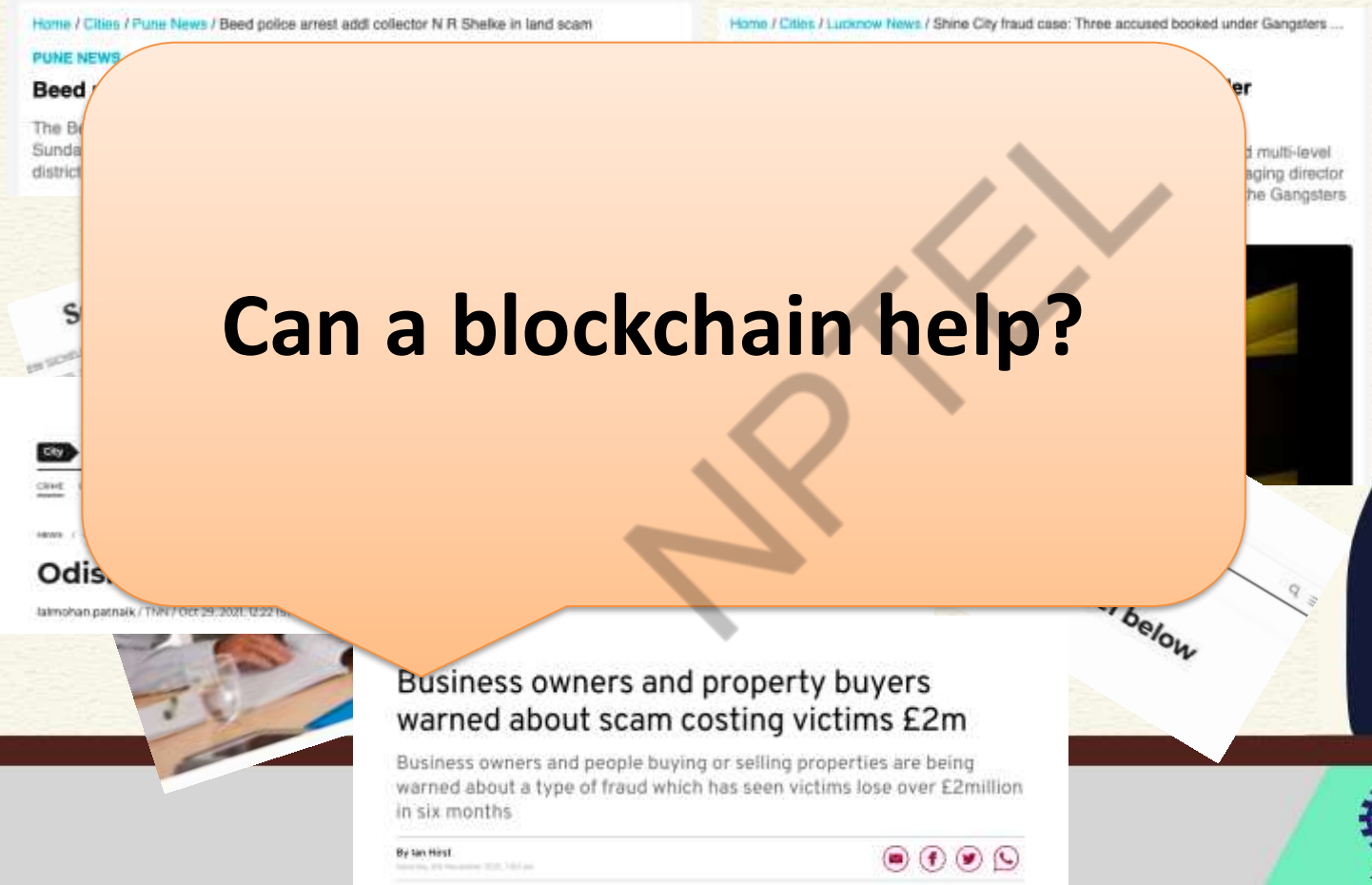
News > Crime

Business owners and property buyers warned about scam costing victims £2m

Business owners and people buying or selling properties are being warned about a type of fraud which has seen victims lose over £2million in six months

By Ian Hirst

Real Estate Scams and Frauds



Can a blockchain help?

Real Estate Scams and Frauds

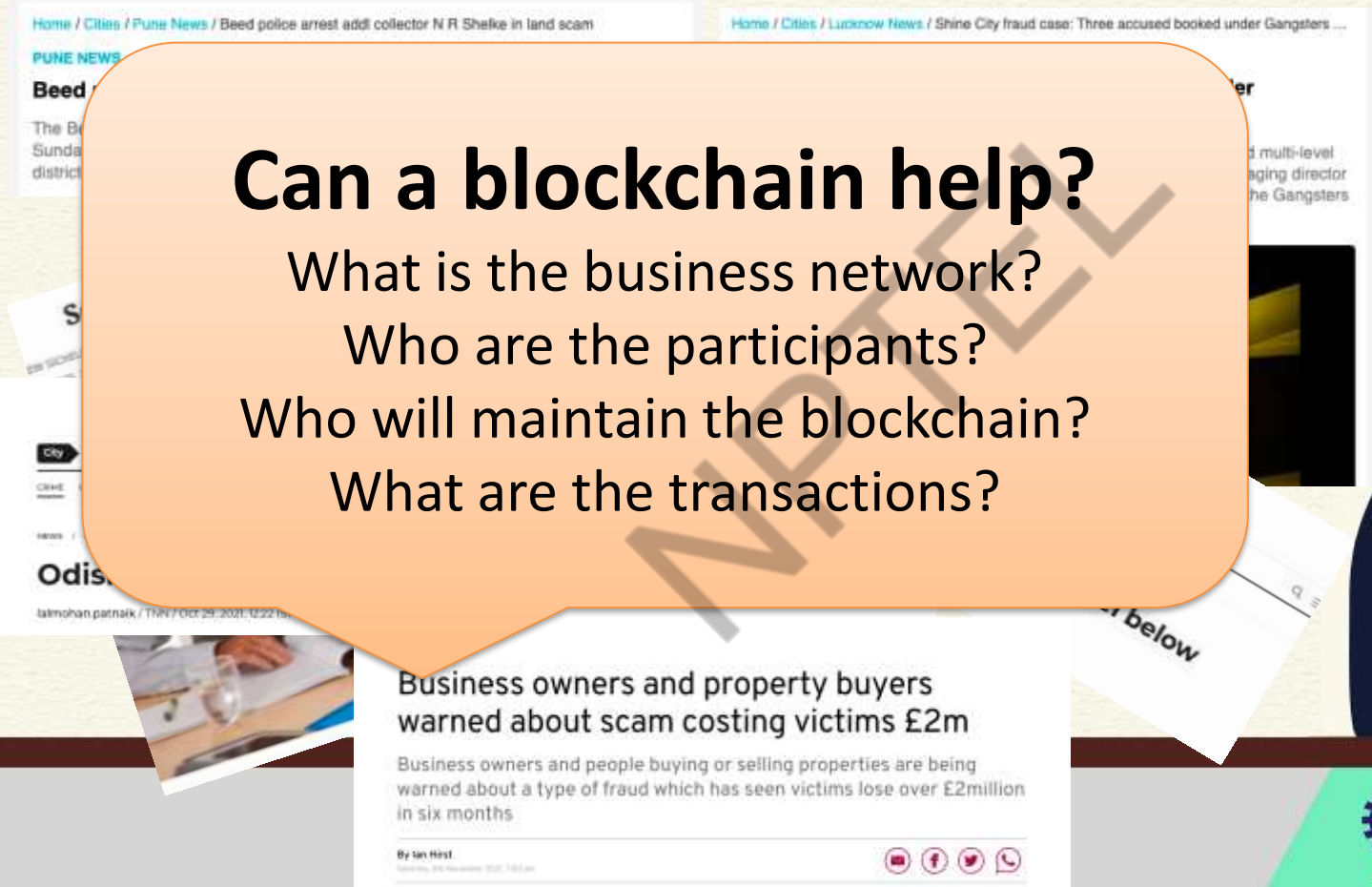
Can a blockchain help?

What is the business network?

Who are the participants?

Who will maintain the blockchain?

What are the transactions?



The People in the Business Network

- Government
- Real estate agents (?)
- Buyers
- Sellers
- Investors (Crowdfunding)
- Startups (real estate business)

The Assets

- Lands
- Properties (buildings, etc.)
- Money

The Transactions

- Buy lands and/or properties
- Sell lands and/or properties
- Crowdfund an investment
- Return from a crowdfunded investment

Public or Private Blockchain

- **Public Blockchain**
  - Pros: Open network, anyone can invest or participate as a startup
  - Cons: You do not know to whom you are investing

Public or Private Blockchain

- **Private Blockchain**
  - Pros: The identity of the participants are known, better security (?)
  - Cons: Who will validate the authenticity? May fallback to a centralized system

Advantages of using blockchain

- Provides a decentralized platforms and marketplace
- Can avoid intermediaries
- Liquidity in business – can be traded readily
- Fractional ownership and crowdfunded investments
- Reduced cost of transactions
- Better transparency

But there are many important implementation questions ...

- Who are going to be the full nodes of the system?
  - Government?
  - Investors?
  - Startups?
  - Buyers, sellers?

But there are many important implementation questions ...

- **Everyone is a full node**
  - I'll sell my property for once … why should I download the entire blockchain?
  - Should I sign out once I am done? How do I resolve a query that comes later on?
    - Do I need to keep my keys forever?
    - What if I loose the keys?

But there are many important implementation questions ...

- **I am not the full node**
  - Which full node should I trust?

But there are many important implementation questions ...

- **Blockchain, by default, is <u>world-readable</u> and <u>world-writable</u>**
  - Isn't it a privacy concern?
  - Say, I am an investor. Everyone can see where I have invested and how much money I have invested

But there are many important implementation questions ...

- **Blockchain, by default, is world-readable and world-writable**
  - Isn't it a privacy concern?
  - Say, I am an investor. Everyone can see where I have invested and how much money I have invested
    - Cross-argument: Use keys to secure the channel

But there are many important implementation questions ...

- **Blockchain, by default, is world-readable and world-writable**
  - Isn't it a privacy concern?
  - Say, I am an investor. Everyone can see where I have invested and how much money I have invested
    - Cross-argument: Use keys to secure the channel
      - Who is going to provide the key?

But there are many important implementation questions ...

- **What should be the credential to participate as an investor or a start-up?**
  - Who will validate that a start-up is not a fraud
    - Trusted third party?
      - Then why can't that trusted third party maintain a database?
        - **Note:** There are methods for blind signatures, you don't need to reveal all information to the TTP

Conclusion

- There are many fundamental questions that need to be solved before putting an application to the blockchain
- The application designer needs to analyze all possible trade-offs
  - Is the benefit more than the cost?
- Digitizing the land and property records might solve many of the problems! Need to think of it ...

Conclusion

- We have seen the idea of decentralized identity management
  - Can explore whether that can be coupled with other applications to solve some of the problems that we mentioned

NPTEL ONLINE CERTIFICATION COURSES

Blockchain and its applications

Prof. Sandip Chakraborty

Department of Computer Science & Engineering
Indian Institute of Technology Kharagpur

Lecture 57: Blockchain in Financial Services

CONCEPTS COVERED

- **Cross-border payments over blockchain**
- **Project Ubin**

KEYWORDS

- Steller Protocol and Network
- Ripple Protocol and Network
- Project Ubin

Cross-Border Payments

- Classic use case for which Bitcoin was created and perhaps the holy grail of cryptocurrencies
- To date, we have over 6000 cryptocurrencies!
- But, what qualifies as a currency. In economics, the following criteria must be satisfied:
  - Medium of exchange: Are merchants willing to accept the currency in exchange for goods and services
  - Unit of account: Is it a measure of the real value of goods and services (e.g., would a merchant be willing to accept the same value regardless of relative currency fluctuations)
  - Store of value: A mode of investment

Steller Protocol and Network

- Decentralized, hybrid blockchain platform with open membership; launched in 2014; **Lumens** as native asset
- **Federated Byzantine Agreement** (FBA) – quorums formed based on participants individual trust decisions, followed by agreement within quorums (Steller Consensus Protocol)
- 2-5 second transaction clearance
- Anchors act as bridges between a given currency and Stellar network
- Has a **distributed exchange**: pay in EUR with INR balance and network will automatically convert it at lowest rate for you

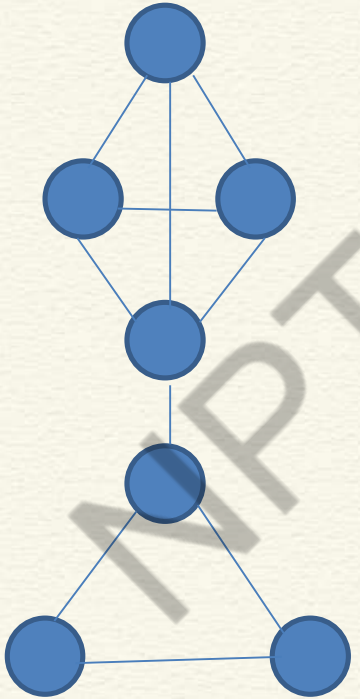
https://www.stellar.org/

Steller Protocol and Network

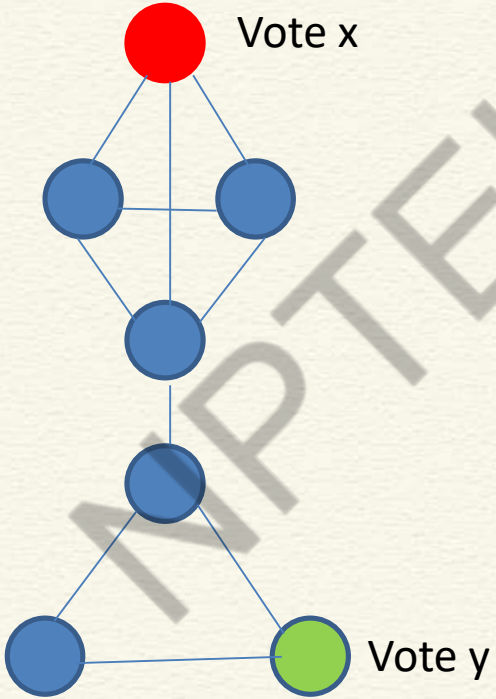
- The idea got published in a SOSP 2019 Paper --
  - Lokhava, Marta, et al. "Fast and secure global payments with Stellar." *Proceedings of the 27th ACM Symposium on Operating Systems Principles*. 2019.

- **Federated voting:** Nodes try to agree on abstract statements by first voting, then accepting, and finally confirming statements.
  - Keep on voting any valid statement (that the nodes believe to be valid)
  - Accept when a majority votes (form quorums)
  - Confirm when the quorum unanimously accepts a statement

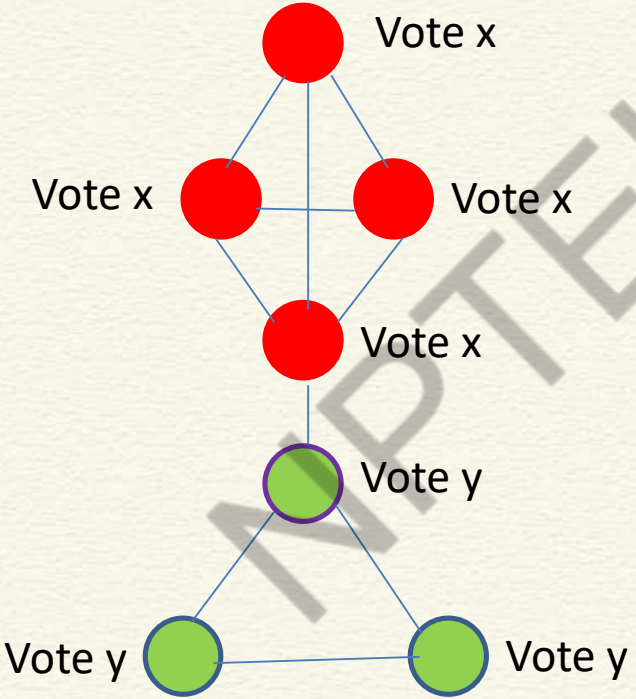
Federated Voting in Steller



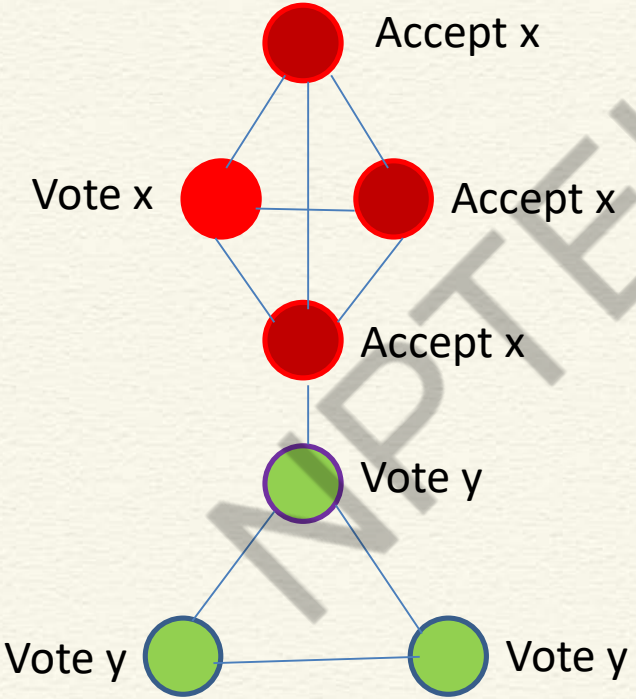
Federated Voting in Steller



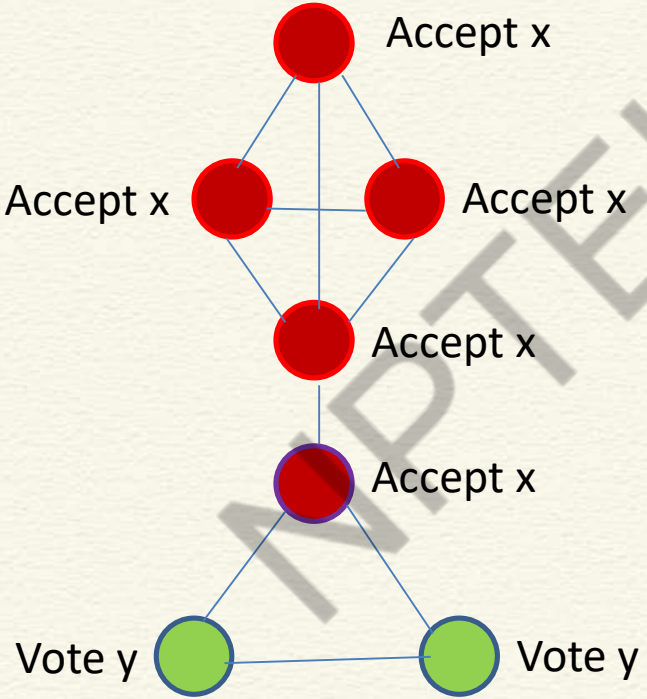
Federated Voting in Steller



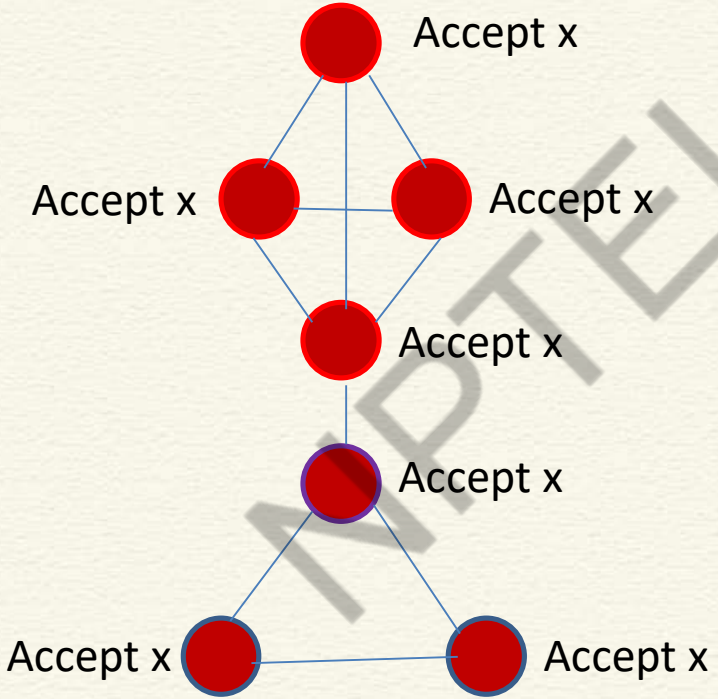
Federated Voting in Steller



Federated Voting in Steller



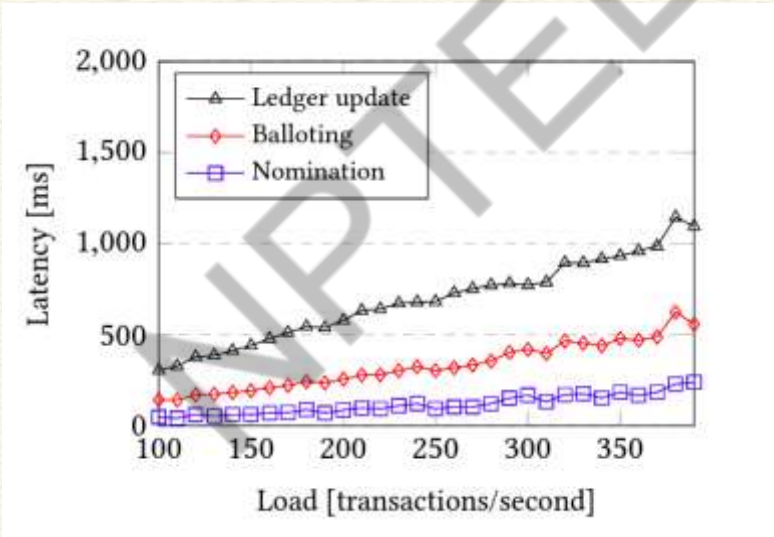
Federated Voting in Steller



Steller Protocol and Network

- Partially synchronous protocol
  - Safety under asynchronous assumptions
  - Liveness require a synchronous network

- **Performance**:



Ripple Protocol and Network

- Protocol for banks to clear and settle payments in real time through a distributed network
- Consensus (**XRP Ledger** – **XRPL** -- https://xrpl.org/) allows payment exchanges and remittance to happen without need for a centralized clearing house
- Average 5 second confirmations; no mining, custom protocol that hasn't yet been validated for correctness and fault tolerance
- Gateway nodes convert fiat currencies to **XRP** (currency in Ripple)
- Market-makers convert from one currency to another
- Centralized governance, with Ripple still holding a large fraction of the cryptocurrency
- https://ripple.com

Ripple Protocol and Network

- Unlike Steller, there are open questions on Ripple consensus
  - Chase, Brad, and Ethan MacBrough. "Analysis of the XRP ledger consensus protocol." *arXiv preprint arXiv:1802.07242* (2018).
  - Claims that XRPL violates safety and liveness

Project Ubin: SGD on Distributed Ledger

- A collaborative project with the industry to explore the use of Blockchain and Distributed Ledger Technology (DLT) for clearing and settlement of payments and securities
  - Taken up by the Monetary Authority of Singapore (MAS) in November, 2016
  - Reports available on the MAS website: https://www.mas.gov.sg/schemes-and-initiatives/project-ubin

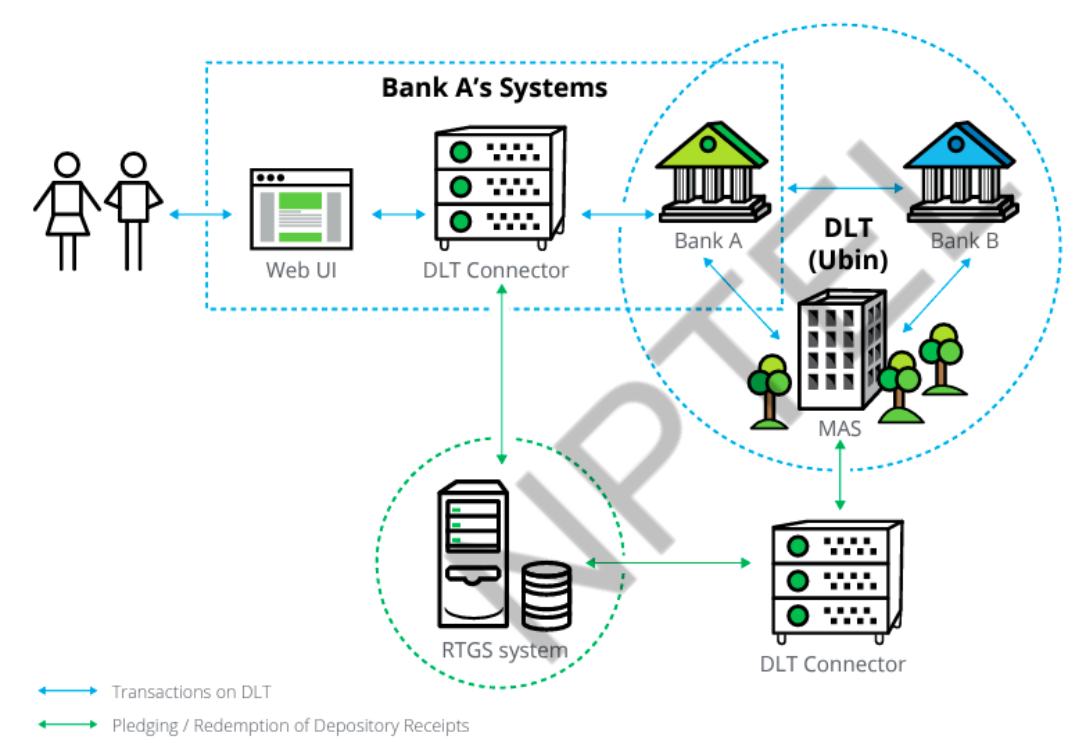
Project Ubin: SGD on Distributed Ledger

- Five-phase project
  - Phase 1: Tokenized SGD
  - Phase 2: Re-imagining RTGS
  - Phase 3: Delivery versus Payment (DvP)
  - Phase 4: Cross-border Payment versus Payment (PvP)
  - Phase 5: Enabling Broad Ecosystem Collaboration

Project Ubin: SGD on Distributed Ledger

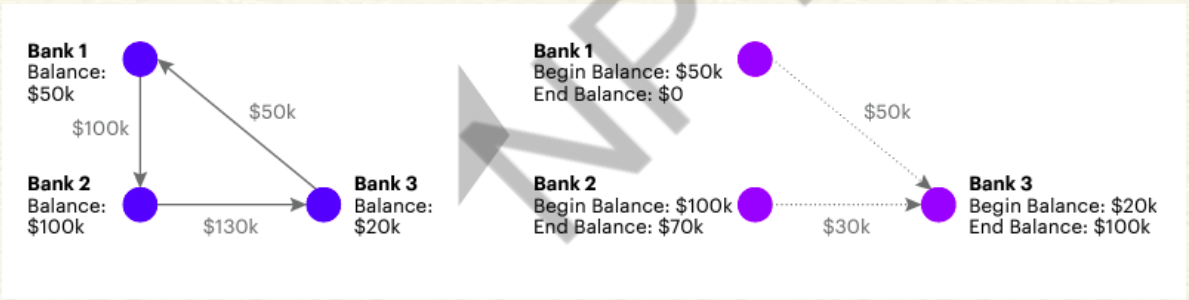
- Phase 1: Tokenized SGD
  - Consortium of financial institutions to conduct inter-bank payments using blockchain technology
    - Bank of America Merrill Lynch, Credit Suisse, DBS Bank, HSBC, JP Morgan, Mitsubishi UFJ, OCBC, R3, Singapore Exchange (SGX), United Overseas Bank
  - Include DLT-based payment in MEPS+
  - Participant banks pledge cash into a custody account held at MAS. MAS will then create the equivalent value in Digital SGD on the DL and assign them to the respective banks.

Project Ubin: SGD on Distributed Ledger



Project Ubin: SGD on Distributed Ledger

- Phase 2: Re-imagining RTGS
  - Led by MAS and The Association of Banks in Singapore (ABS)
  - Developed PoC using three DLT platforms – Ethereum, Fabric, and R3 Corda; open-sourced https://github.com/project-ubin
  - Solves the problem of gridlock

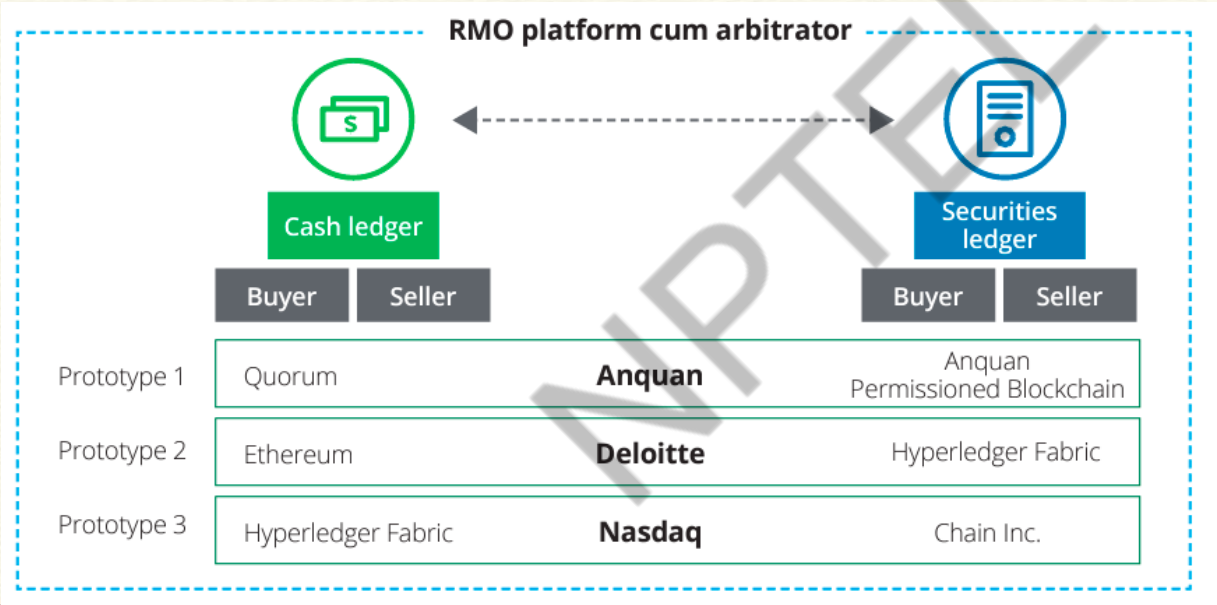


Project Ubin: SGD on Distributed Ledger

- Phase 3: Delivery versus Payment (DvP)
  - The cash payment for a purchased security occurs prior to, or upon, its delivery
    - Two counterparties (traders) meets at an agreed time to exchange the agreed assets.
  - In this phase, MAS and SGX collaborated to realise domestic DvP settlement on two separate blockchain platforms

Project Ubin: SGD on Distributed Ledger

- Phase 3: Delivery versus Payment (DvP)

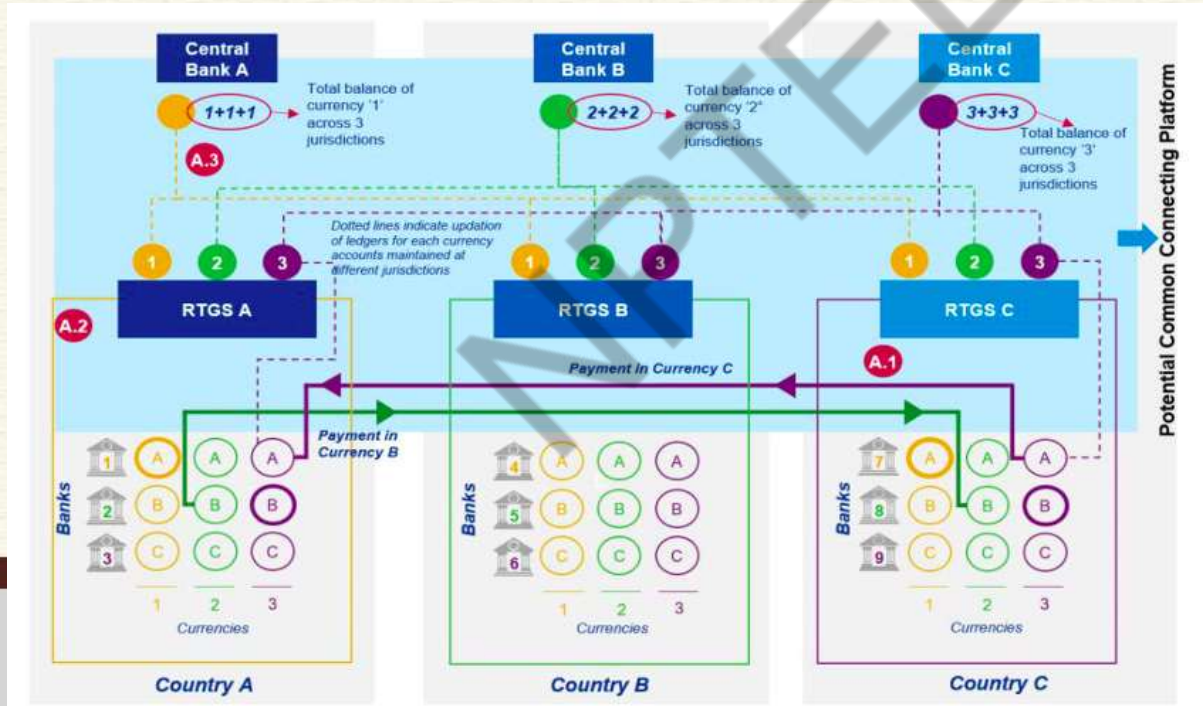


Project Ubin: SGD on Distributed Ledger

- Phase 4: Cross-border Payment versus Payment (PvP)
  - Joint initiative by Bank of Canada (BoC), Bank of England (BoE) and MAS; initiated in November, 2018
  - Transparency in payment status, availability of cross-border payment services, reduced time for payment processing, reduced costs
  - Considers three different payment models and analyzes their respective impact and scale

Project Ubin: SGD on Distributed Ledger

- Phase 4: Cross-border Payment versus Payment (PvP)
  - **Model 2**

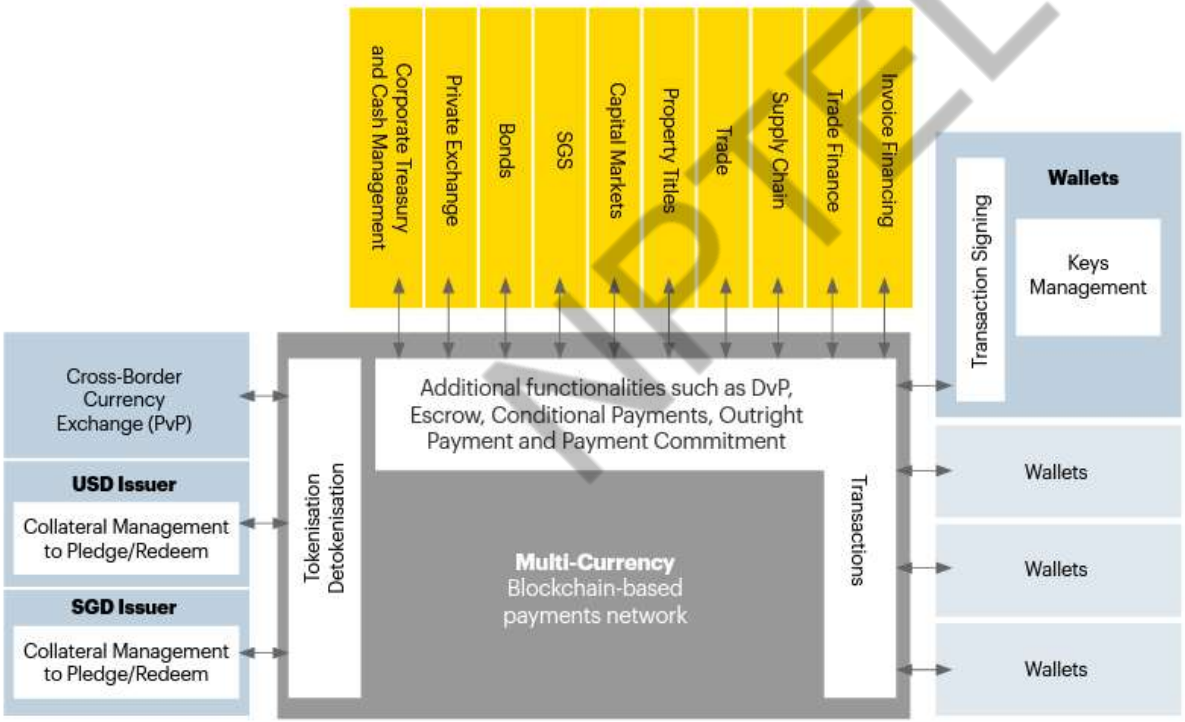


Project Ubin: SGD on Distributed Ledger

- Phase 5: Enabling Broad Ecosystem Collaboration
  - Provides technical insights into the blockchain-based multi-currency payments network prototype that was built
    - Describes how the network could benefit the financial industry and blockchain ecosystem.

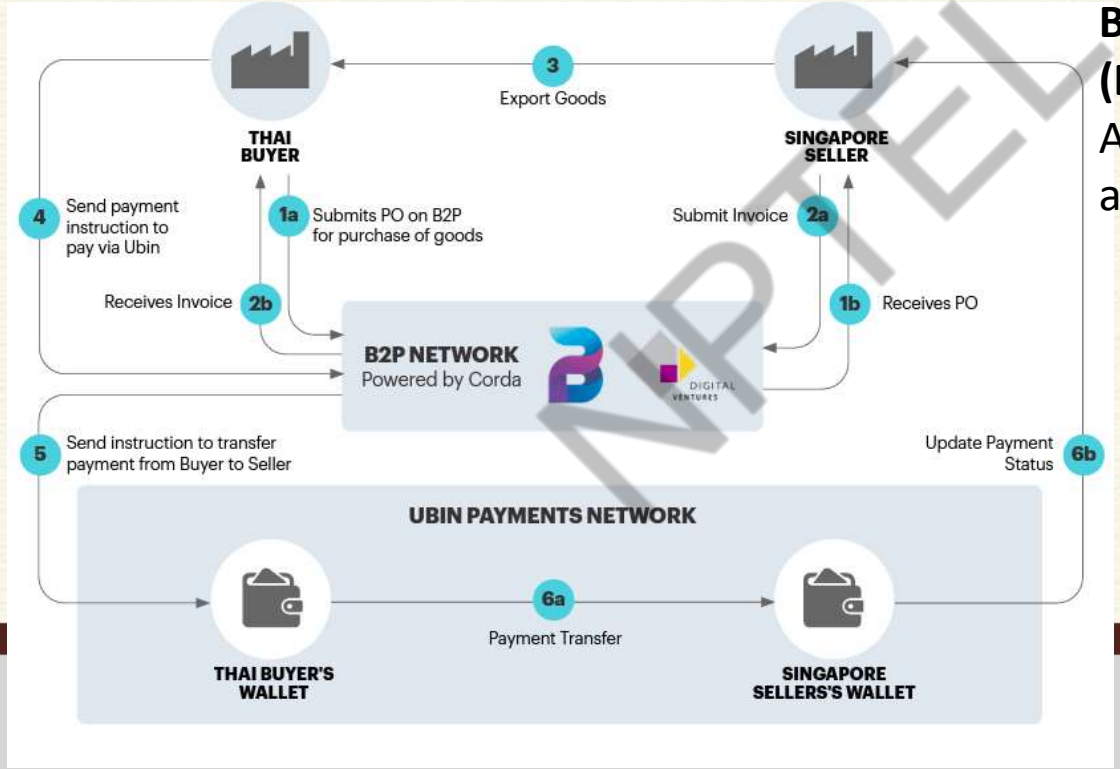
Project Ubin: SGD on Distributed Ledger

- Phase 5: Enabling Broad Ecosystem Collaboration



Project Ubin: SGD on Distributed Ledger

- Phase 5: Enabling Broad Ecosystem Collaboration



Blockchain for Procure-to-Pay (B2P)

Automated document verification and payment processing

Conclusion

- Financial services have been one of the key use-cases for Blockchain
- Project Ubin develops a payment network prototype for multi-currency payments; the project has been open-sourced
- Check the project reports for Ubin: https://www.mas.gov.sg/schemes-and-initiatives/project-ubin

NPTEL ONLINE CERTIFICATION COURSES

Blockchain and its applications

Prof. Sandip Chakraborty

Department of Computer Science & Engineering
Indian Institute of Technology Kharagpur

Lecture 58: Public Sector Use Cases

CONCEPTS COVERED

- **Government use cases of blockchain**

KEYWORDS

- Public data management
- Public taxation
- National strategies

Blockchain and Government

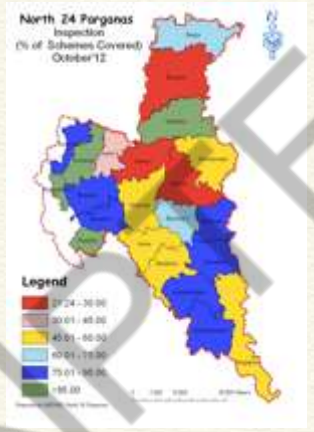
- Government needs to maintain (in digital or in paper form)
  - Daily operations and activities
  - Government assets (land records, buildings etc.)
  - Details of people, organizations and institutions
  - Records of people
  - Business transactions

Multi-institutional and Multi-Organizational

- Different levels of governance

Country

State



District

Village, Panchyat, Cities

Multi-institutional and Multi-Organizational

- Every level builds its own ledger of data
  - Different access management policies
  - Role based access control or access management

- Different priority of data
  - High priority or highly secured data - restricted access - needs to prevent from unauthorized access (example: AADHAAR Data)

Blockchain and Government

- Blockchain can help in management of government data at different levels

- **Note**
  - Directly store the data on blockchain?
  - The data cannot be altered without colluding majority of the blocks
  - Data access as transactions - can check or verify who has accessed what

Government and Cyber Crime

- Government database is a major target for hackers
  - In 2020, there are 1001 cases of data breaches that affected 155.8 million individuals (Source: https://www.statista.com/)

- **"Cyber War" -** actions by a nation-state to penetrate another nation's computers or networks (*Richard Clarke*)

Theft of Government Data

Nfld. & Labrador

N.L. patient, employee data stolen in health-care cyberattack

Hackers were able to access the information th

News / LATEST / Economy / Info of 4.39 cr investors exposed
arm: CyberX9

Info of 4.39 cr investors exposed twice within 10 days due to data breach at CDSL's KYC arm: CyberX9

The Central Depository Services (India) Limited (CDSL) is a Sebi registered depository and CDSL Ventures Ltd is a KYC registering agency separately registered with Sebi.

Home > News > Security > FBI warns of fake govt sites used to steal financial, personal data

FBI warns of fake govt sites used to steal financial, personal data

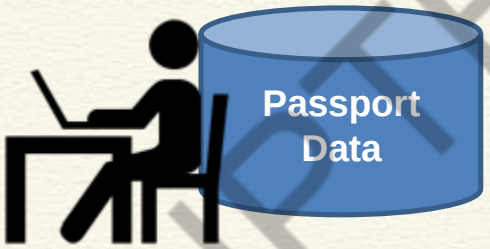
By **Sergiu Gatlan**

October 19, 2021 09:00 AM 0

Processing of Government Data

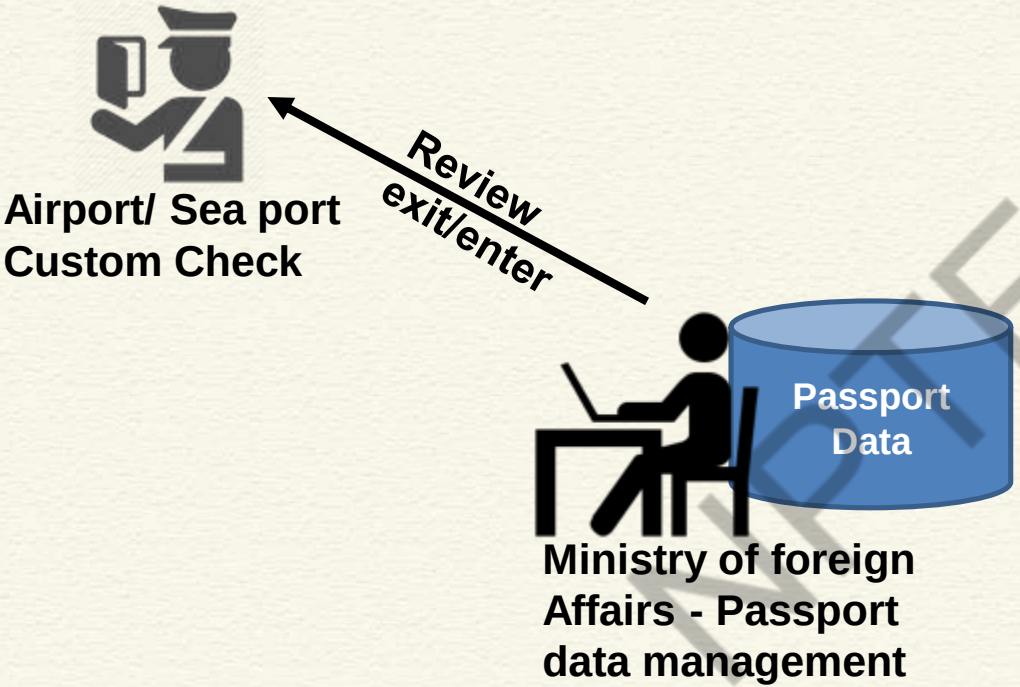
- Data is shared among multiple organizations at different level of government structure
- The problem of data breaches increases at every level
  - Data duplication
  - Data multiplicity
- Protection of data gets diluted if multiple copies of same data exist

Sharing of Passport Data: An Example

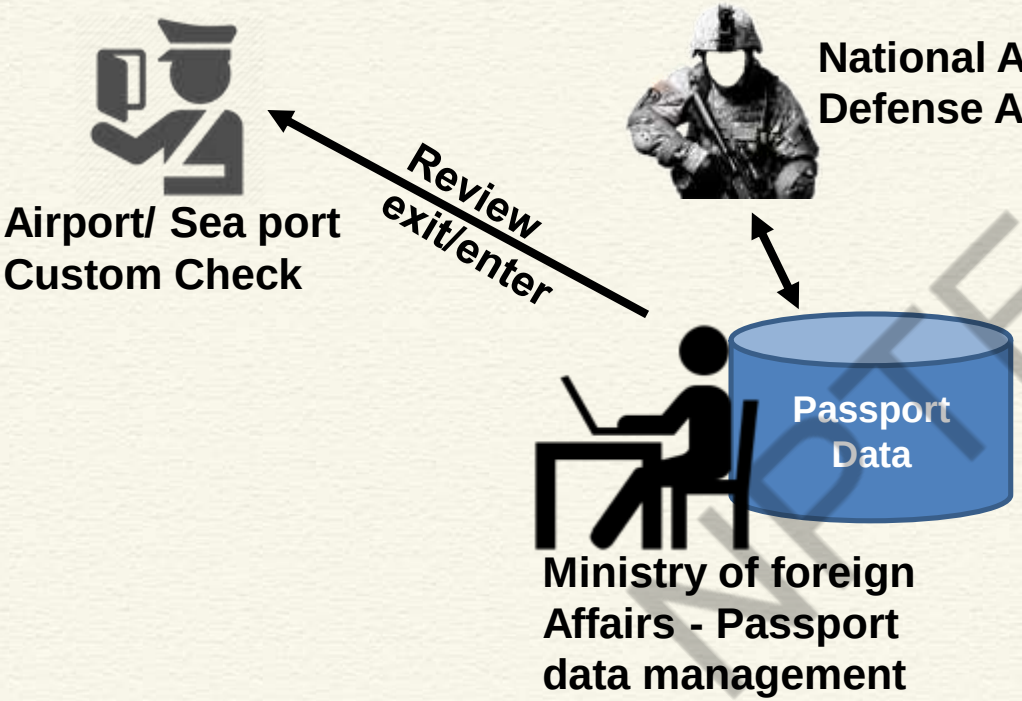


Ministry of foreign Affairs - Passport data management

Sharing of Passport Data: An Example



Sharing of Passport Data: An Example



Sharing of Passport Data: An Example

Airport/ Sea port
Custom Check

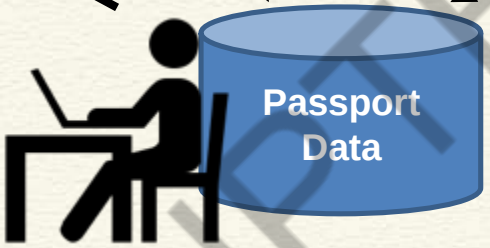
Review
exit/enter

National Army
Defense Agency

Investigation

National Police Agency
CBI/CID - Crime department

Public Service
Identity Database



Ministry of foreign
Affairs - Passport
data management

Sharing of Passport Data: An Example

Airport/ Sea port
Custom Check

Review
exit/enter

National Army
Defense Agency

Investigation

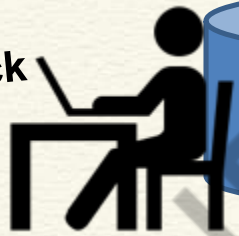
National Police Agency
CBI/CID - Crime department

Public Service
Identity Database

Passport
Data

Periodic Check

Income Tax Department
National Intelligence
National Audit Agency



Ministry of foreign
Affairs - Passport
data management

Sharing of Passport Data: An Example

Airport/ Sea port
Custom Check

Review
exit/enter

National Army
Defense Agency

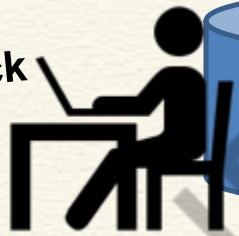
Investigation

National Police Agency
CBI/CID - Crime department

Public Service
Identity Database

Periodic Check

Income Tax Department
National Intelligence
National Audit Agency

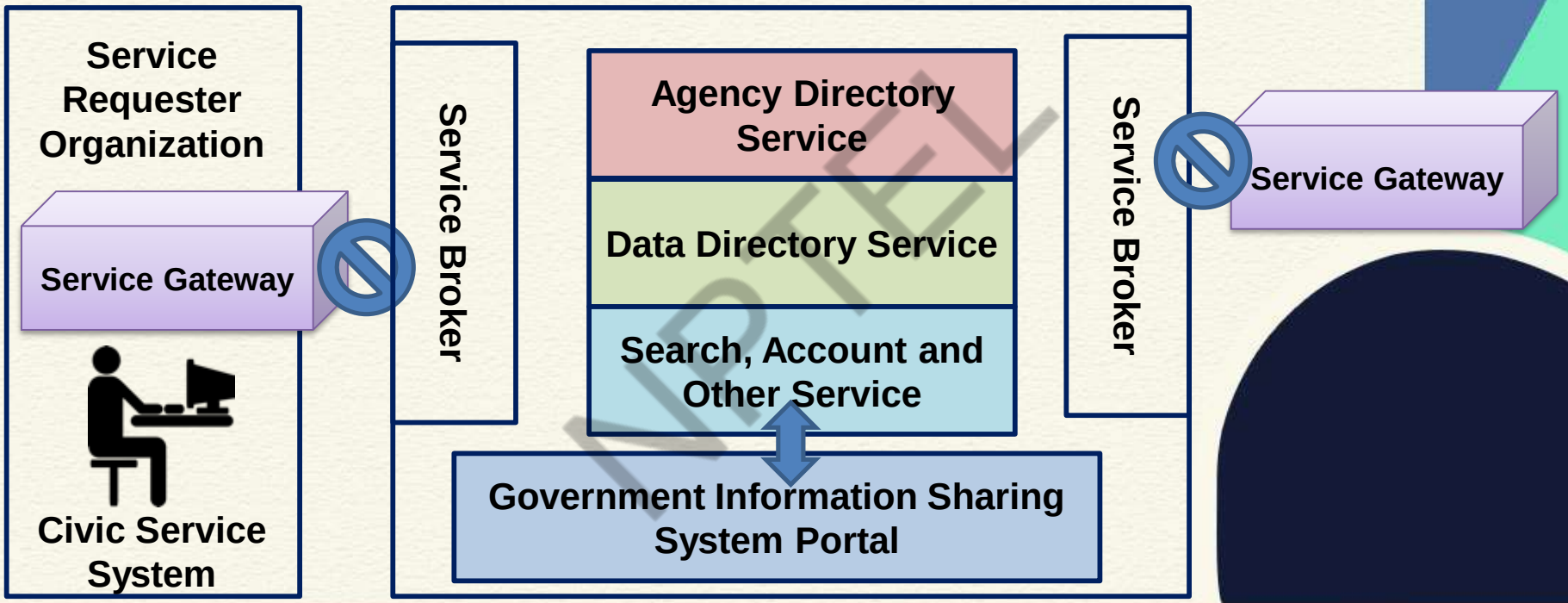


Passport
Data

Ministry of foreign
Affairs - Passport
data management

Ministry of
Public Service

Government Information Sharing System: A Typical Example



How Blockchain Helps

- **Access and verification of a central data**
  - Data is in a central database
  - Access to the database are the transaction
  - Every such transactions (access to the data) is logged in a blockchain
  - Data can be accessed **only** through the blockchain
  - Anyone can verify who has accessed data and for what purpose

How Blockchain Helps

- **Sharing of data**
  - Data is in the blockchain
    - **(May not be the ideal solution all the time)**
  - Everyone can verify which data has been shared
  - Data cannot be altered

How Blockchain Helps

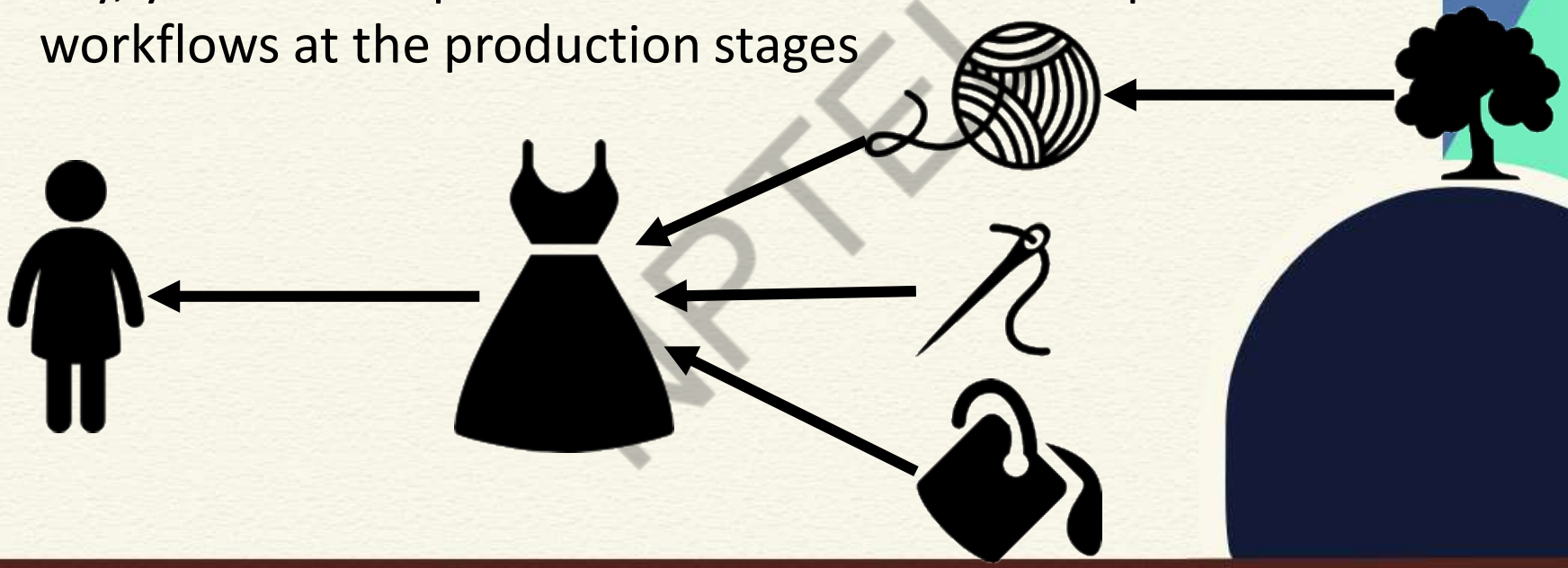
- **Sharing of data and access control**
  - Keep both the data and the access at a blockchain
    - **Depends on the size of the data**
  - Anyone can verify the data and the access
  - Neither data nor access can be altered
  - Access cannot be denied

Case Study: Processing Tax Payments

- Goods and Services Tax (GST) - indirect tax covering various goods and services during the production and service stages
  - IGST
  - SGST
  - CGST
- The entire workflow is pretty complex -
  Let’s see how Blockchain can help!

Case Study: Processing Tax Payments

- Say, you want to purchase a dress - it has multiple workflows at the production stages

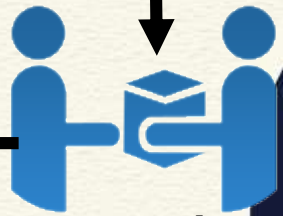


GST without Blockchain

A GST Invoice is issued by the seller

Buyer pays the bill with GST

Information of the payment is recorded at GST Portal



Seller pays to the suppliers

Final Tax goes to the government

Additional payment is adjusted

GST with Blockchain

A GST Invoice is issued by the seller

Buyer pays the bill with GST

Seller pays to the suppliers

Smart Contract adjusts the tax calculation during the payment

Final Tax goes to the government

Case Study: Processing Tax Payments

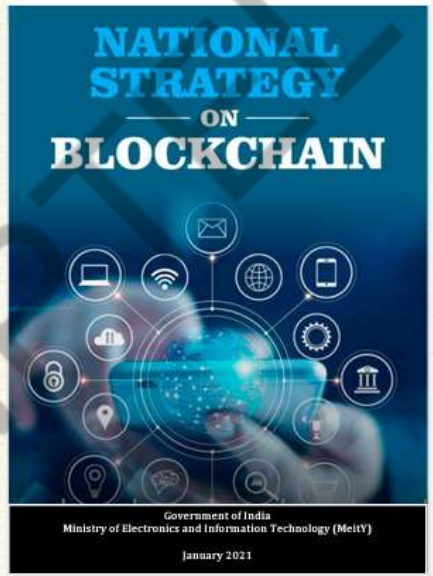
- During the payment for a good or a service
  - Blockchain smart contracts can calculate the invoice based on the tax amount that is already levied during the production process
  - Smart contract directly transfers the tax amount to tax authority (CGST or SGST)
  - The refund, if any, is directly paid to the customer's account

Advantages of using Blockchain

- The administrative burden for accounting services is drastically reduced
- All the transactions are done in real time, no “return filing” is required, or “return filing” can be avoided
- All the transactions are transparent
  - Reduces risk of fraud and mistakes
  - Immediate auditing from the transaction log

Draft National Strategy of Blockchain in India

- Published by **Ministry of Electronics and Information Technology (MeiTY)** during January 2021



Draft National Strategy of Blockchain in India

- Highlights a number of use cases for possible national interests
    - Transfer of Land Records (Property Record Management)
    - Digital Certificates Management (Education, Death, Birth, agreements, sale deeds …)
    - Pharmaceutical supply chain
    - e-Notary Service (Blockchain enabled e-Sign Solution)
    - Farm Insurance
    - Identity management
    - Power distribution
    - Duty payments

Draft National Strategy of Blockchain in India

- Highlights a number of use cases for possible national interests
    - Agriculture and other supply chains
    - eVoting
    - Electronic Health Record Management
    - Digital Evidence Management System
    - Public Service Delivery
    - IoT Device Management and Security
    - Vehicle lifecycle management
    - Chit fund operations administration
    - Microfinance for Self-Help Groups

Draft National Strategy of Blockchain in India

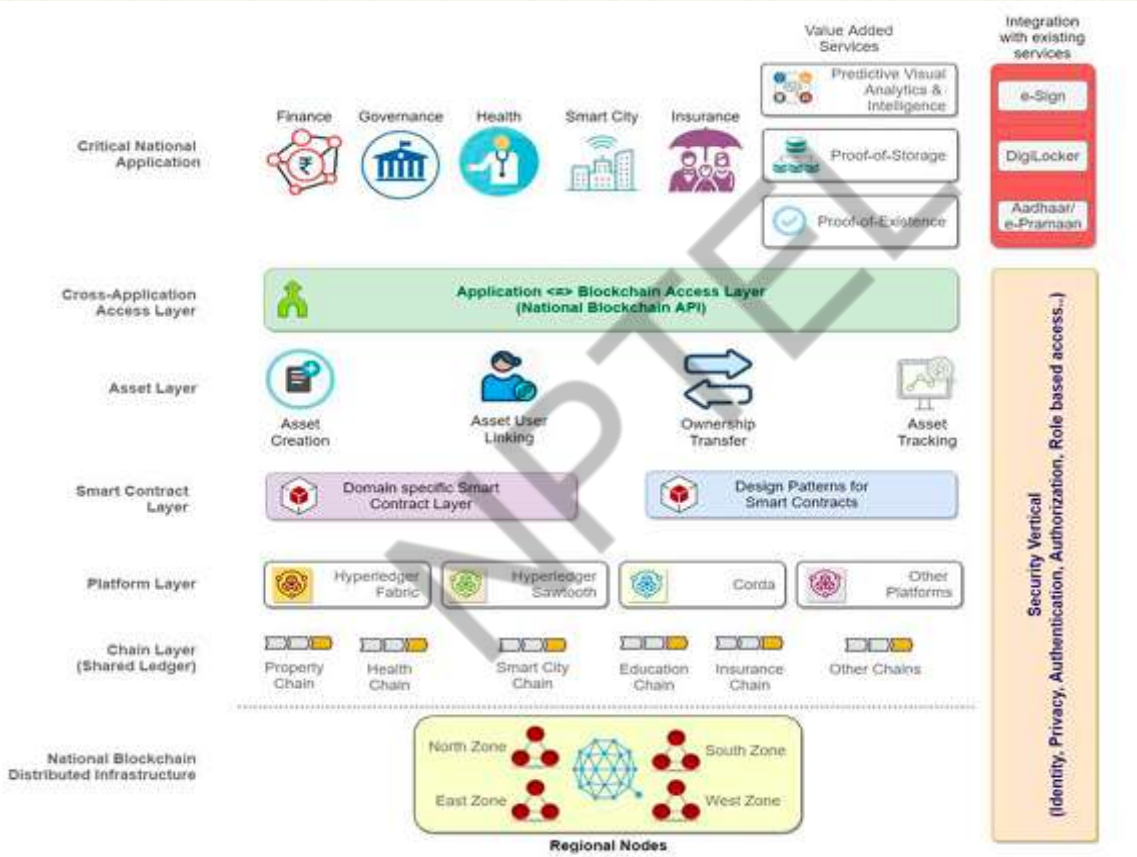
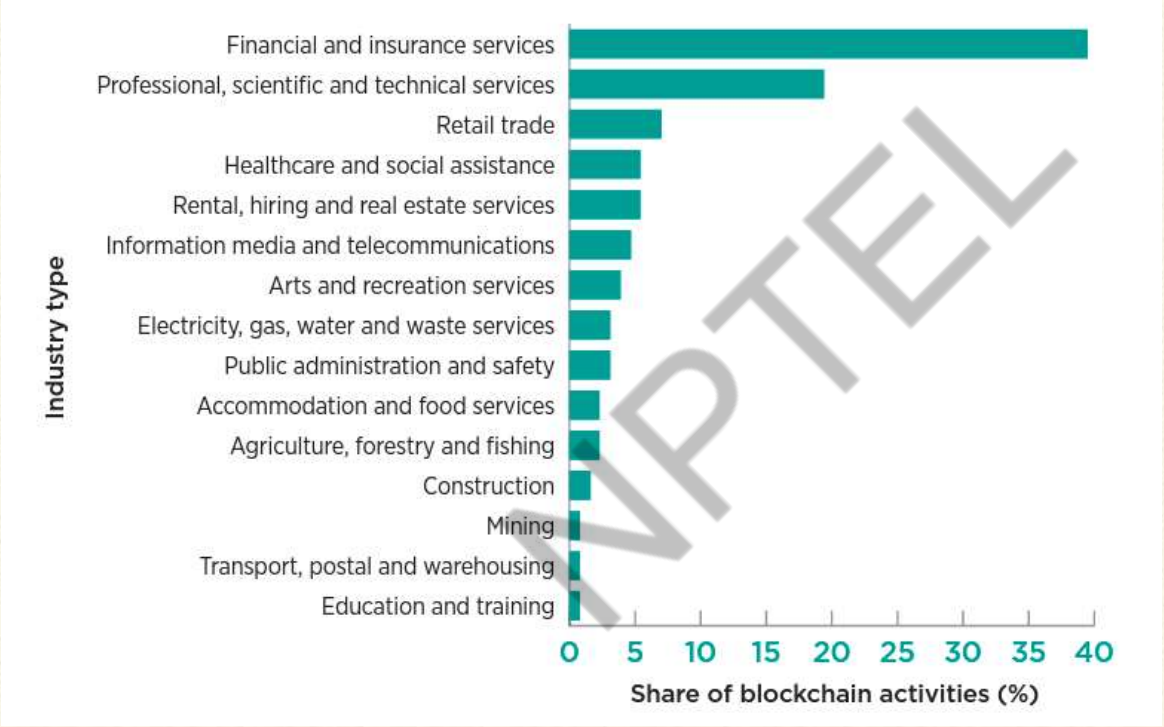


Figure 8: A National Level Blockchain Framework

National Blockchain Roadmap, Australia



Conclusion

- There are various scopes for applying blockchains in public services that involve multiple stakeholders
  - Are we sufficiently prepared?

- However, we should be careful about the possible side channels

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

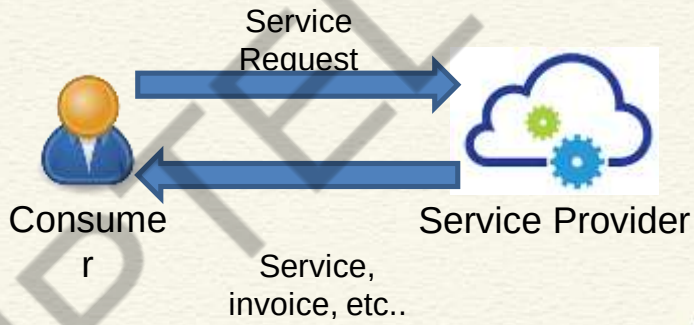
- **Blockchain application for a decentralized marketplace**

KEYWORDS

- **Design a blockchain use-case**
- **Analyzing the requirements**

Online Service Providers

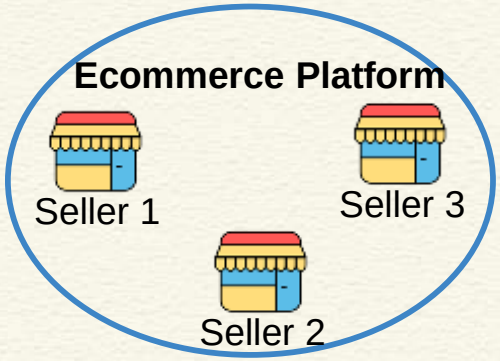
- Offers services to the consumers (end-users).
- Use web interface or mobile apps for communicating with consumers.
- Examples:
  - Ecommerce
  - Cloud Service Providers
  - Media Service Providers
  - Logistics Providers

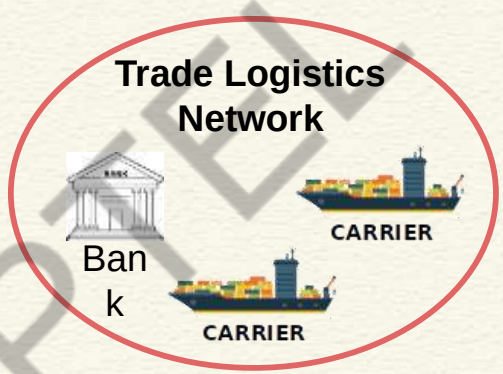


Online Service Providers

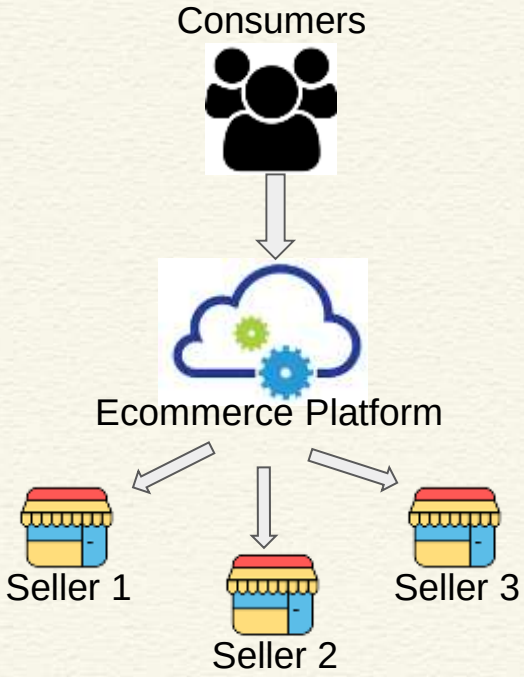
- Multiple service providers (SPs) come into agreement to collaborate.
- Gain access to the common larger set of end-users.
- Offer wider range of services under the same platform.
- Meet user demands by sharing resources.
- Examples:
  - Different sellers under **ebay**, **Amazon**.
  - Cloud infrastructure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

Online Service Providers



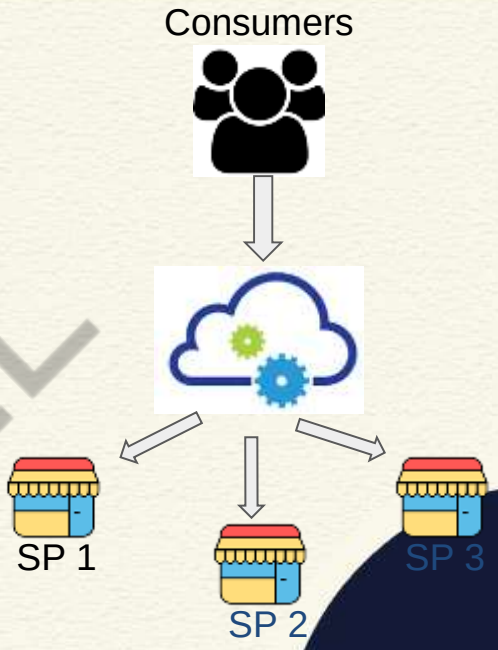


Existing Consortia -- Centralized



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.

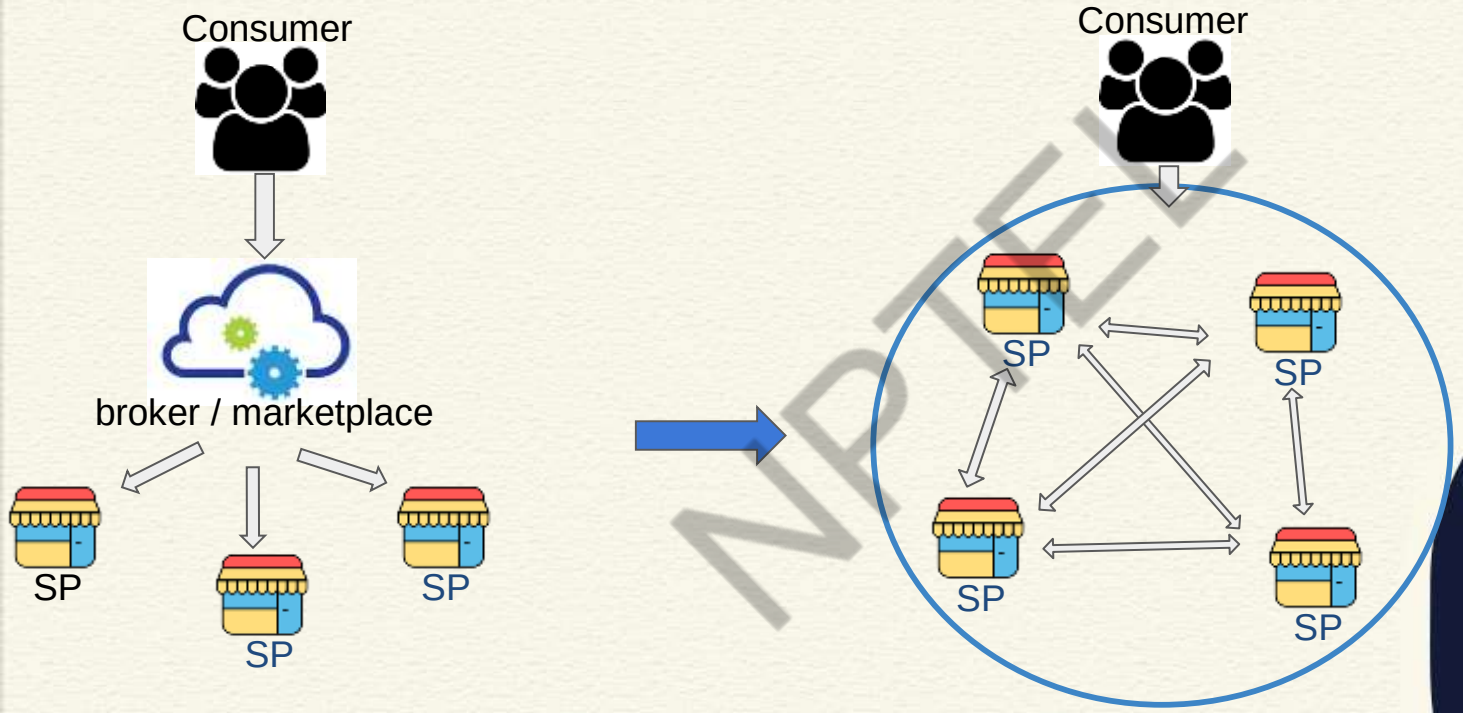
Objective

- 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].

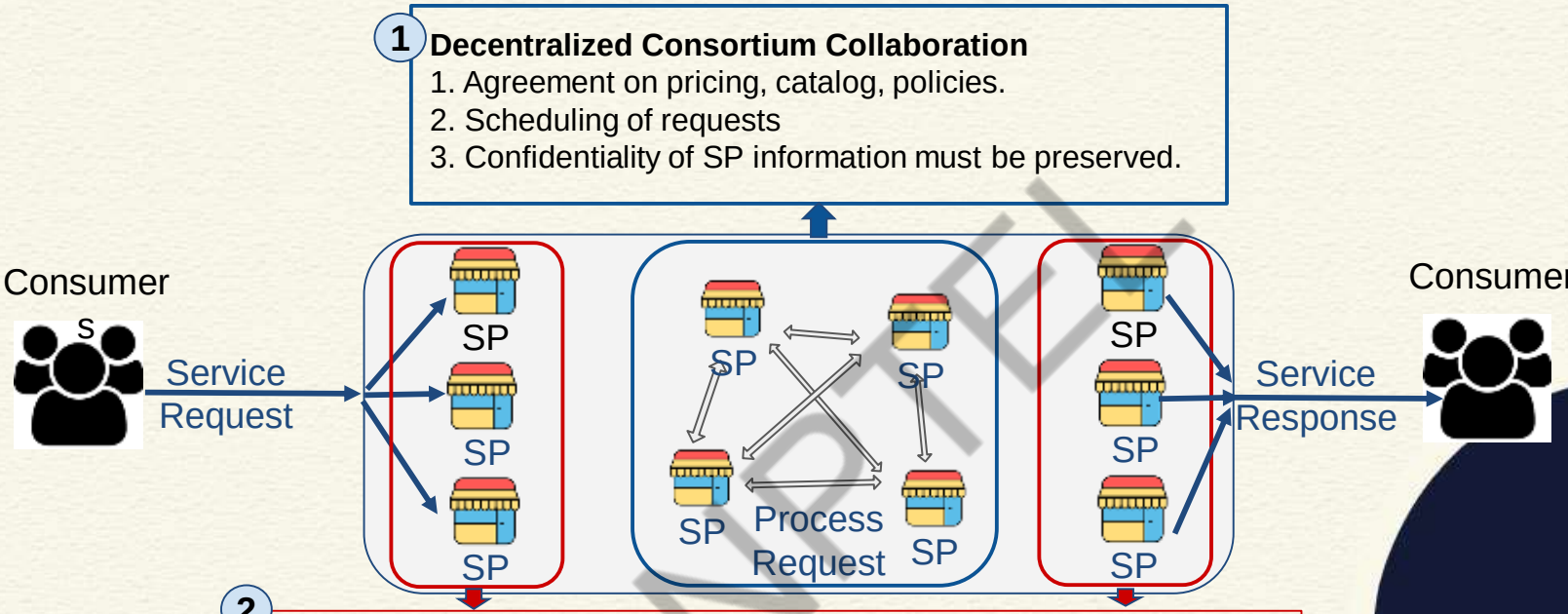
C. Verifiability and confidentiality of information from the consortium

- 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.

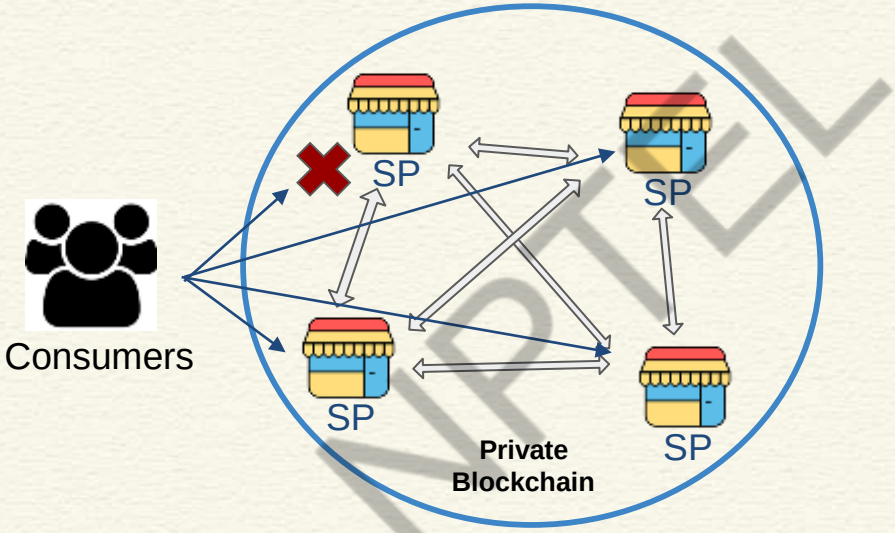
Threat Models

- **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.

1. **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

Consumers

Service Request Contract

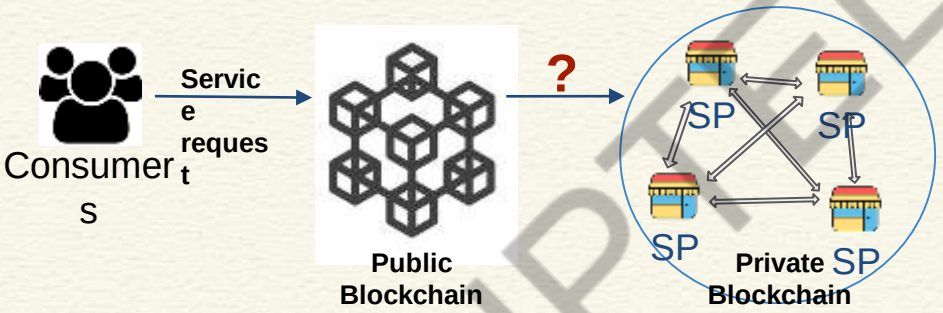
Service request - smart contract execution transaction

Tx Propagation:
Tx is flooded among the participants

Block Mining:
Block is mined based on PoW / PoS / other.

Block Confirmation:
Mined block is flooded in the network.

Transferring Consensus to the Consortium

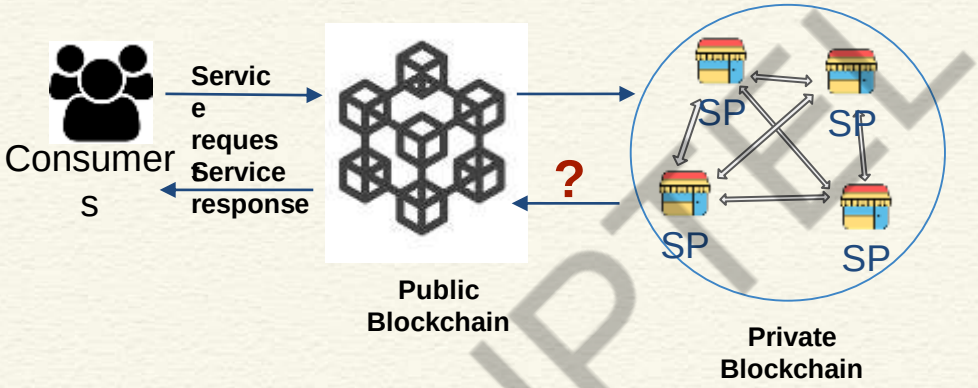


Transferring Consensus to the Consortium

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.

NPTEL ONLINE CERTIFICATION COURSES

Blockchain and its applications

Prof. Sandip Chakraborty

Department of Computer Science & Engineering
Indian Institute of Technology Kharagpur

Lecture 60: Blockchain for Decentralized Marketplace (Part 2)

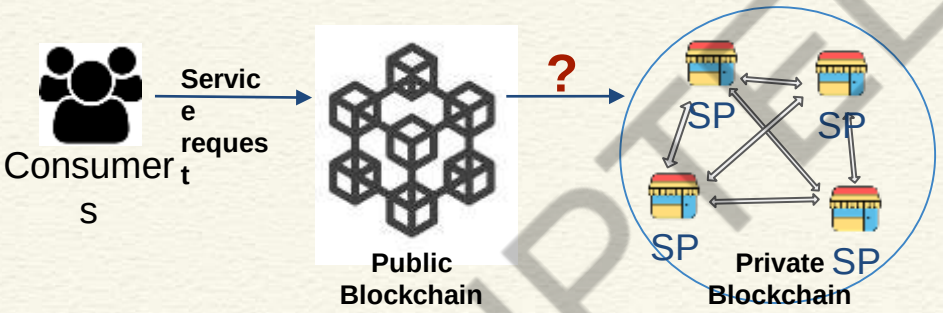
CONCEPTS COVERED

- **Blockchain application for a decentralized marketplace**

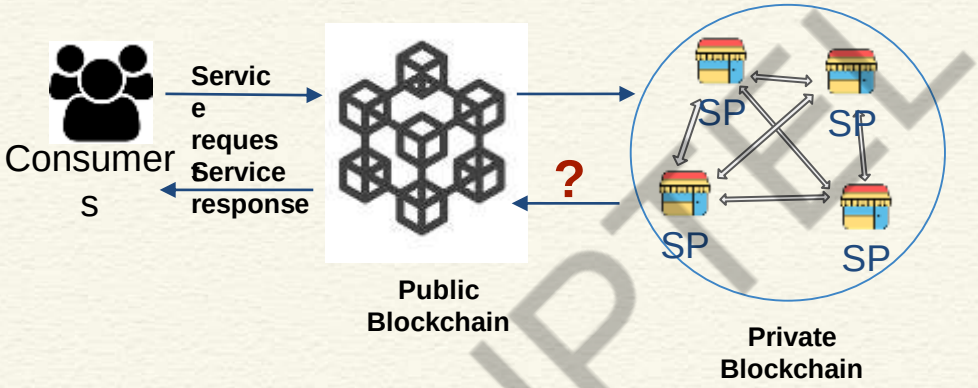
KEYWORDS

- Design a blockchain use-case
- Analyzing the requirements
- Consensus on Consensus

Transferring Consensus to the Consortium



Transferring Verifiable Response

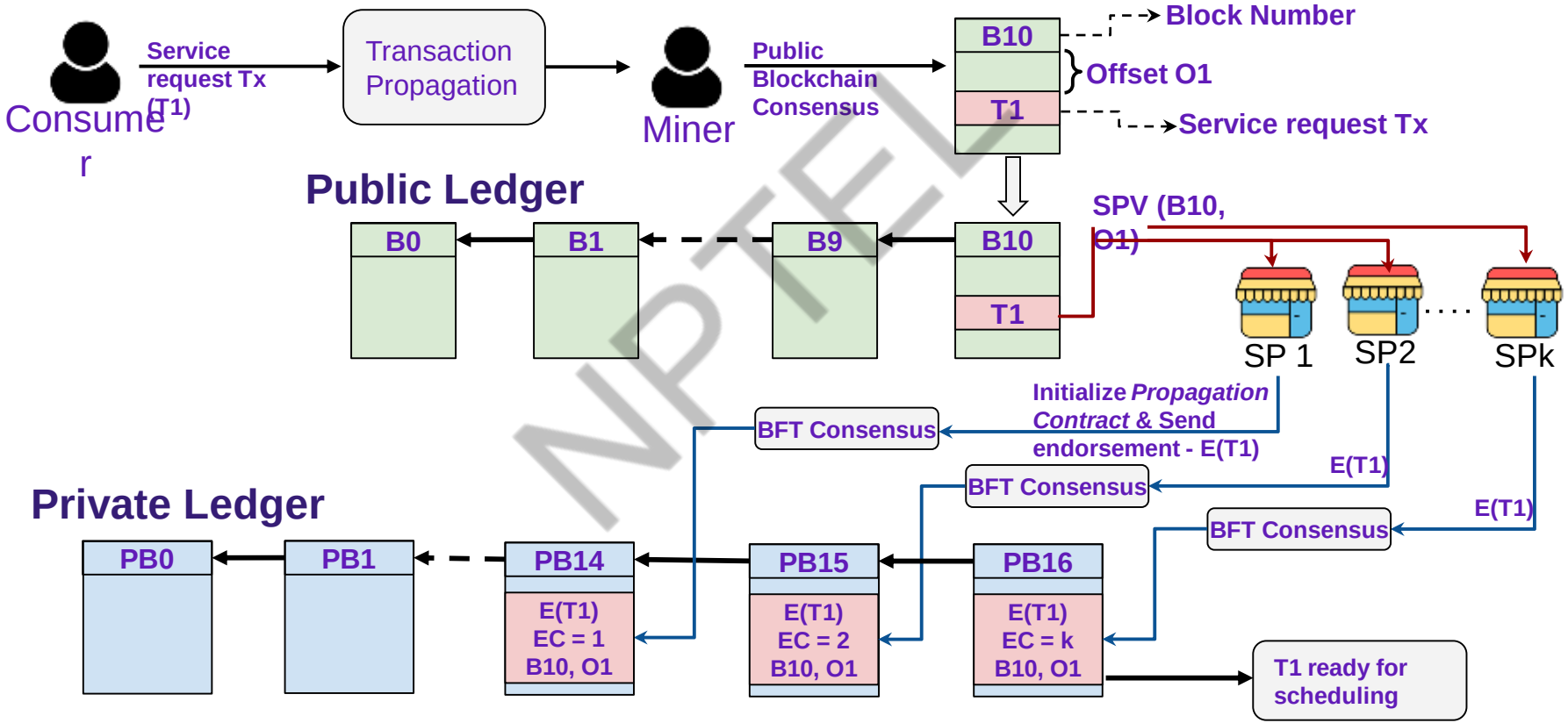


Consensus on Consensus

Consensus propagation from public blockchain to private consortium blockchain

- Each **SP also participates in the public blockchain** to receive service requests from consumers.
- When a transaction is committed in the public ledger, it is verified by the SPs through *Simplified Payment Verification (**SPV**)*[8]
- For each service request, the SPs **collect endorsements** through *Propagation Contract*
- Each endorsement goes through BFT consensus.
- When a service request receives $k \geq \frac{2}{3}$ of the SPs' endorsements, it is marked as confirmed.

Consensus on Consensus



Verifiable Response Transfer

- Two kinds of information need to be transferred from the consortium to the consumers:

a. Consortium information such as catalog, pricing, etc.. - **not sensitive**
b. Request responses - results of scheduling and processing consumer requests such as a digital document, e.g., access credentials, tickets, invoices, etc. - **sensitive**

- Both kinds of data are generated collectively by SPs through private blockchain's consensus process.
- Consumers being outside the permissioned network cannot verify the correctness of the data.
- Separate protocol required for validation of consortium response by consumers.

Verifiable Response Transfer

- We use the concept of Collective Signing (CoSi) [21]
  - A set of consortium **SPs collectively sign** a valid data to make it verifiable.
  - We utilize **Boneh-Lynn-Shacham (BLS)** cryptosystem for **aggregating** signatures from individual SPs.
  - A BLS signature for message $\mathcal{M}$ is computed as: $\mathbb{S}_i(\mathcal{M}) = \mathcal{H}(\mathcal{M})^{\mathcal{S}c_i}$
    - $\mathcal{H}(.)$ is a cryptographic hash function.
    - $\mathcal{S}c_i$ Is secret key of SP $\mathcal{C}_i$

Aggregated multi signature for n SPs:

$$\mathbb{S}_{1..n}(\mathcal{M}) = \mathcal{H}(\mathcal{M})^{\mathcal{S}c_1+\mathcal{S}c_2+..+\mathcal{S}c_n} = \prod_{i=1}^{n} \mathcal{H}(\mathcal{M})^{\mathcal{S}c_i}$$

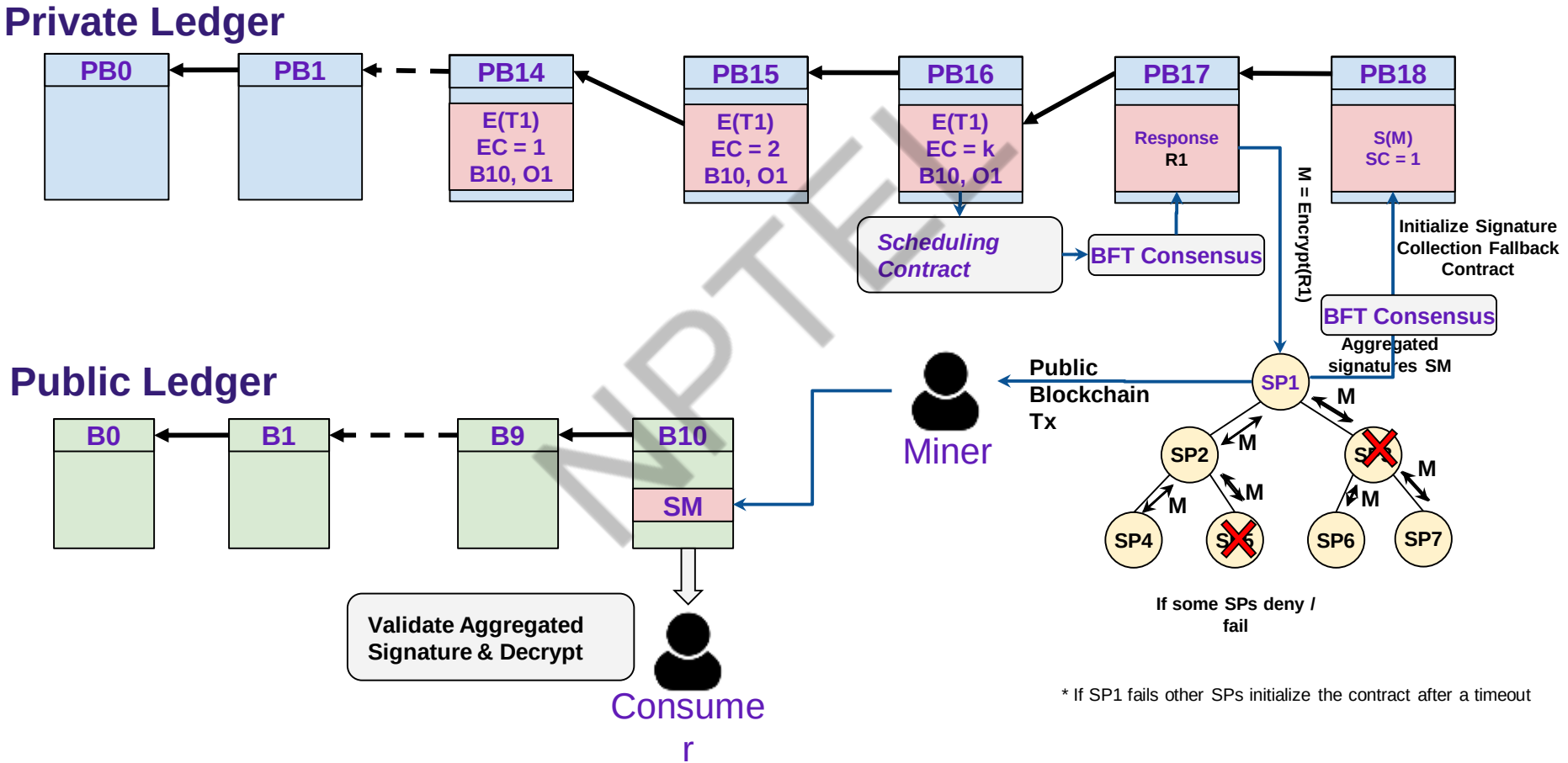
$$= \mathbb{S}_1(\mathcal{M}) \times \mathbb{S}_2(\mathcal{M}) \times .. \times \mathbb{S}_n(\mathcal{M}) = \prod_{i=1}^{n} \mathbb{S}_i(\mathcal{M})$$

[21] Syta, Ewa, Iulia Tamas, Dylan Visher, David Isaac Wolinsky, Philipp Jovanovic, Linus Gasser, Nicolas Gailly, Ismail Khoffi, and Bryan Ford. "Keeping authorities" honest or bust" with decentralized witness cosigning." In 2016 IEEE Symposium on Security and Privacy

Verifiable Response Transfer

- Consortium response is accepted as **valid only if it has ≥ ⅔ of the SPs' signatures**.
- For preserving confidentiality, a response to a consumer is encrypted using its public key.
- **Signature Collection:**
  - Multisignature collection is carried out **off-chain** to improve latency.
  - A **communication tree** is formed along which the singing request and the signatures are exchanged.
  - Each node of the tree aggregates signatures collected from its descendants.
  - **Fallback** to smart contract based signature collection in case of denial of service attack by some SP.

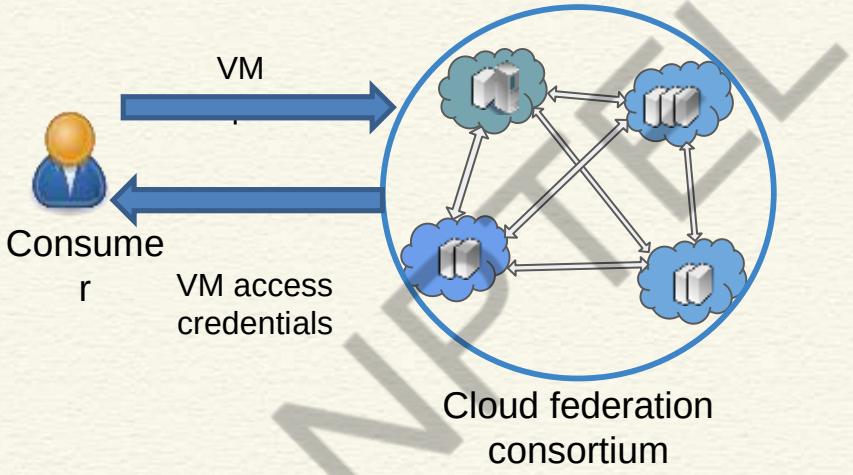
Verifiable Response Transfer



Use Case Implementation: Cloud Federation

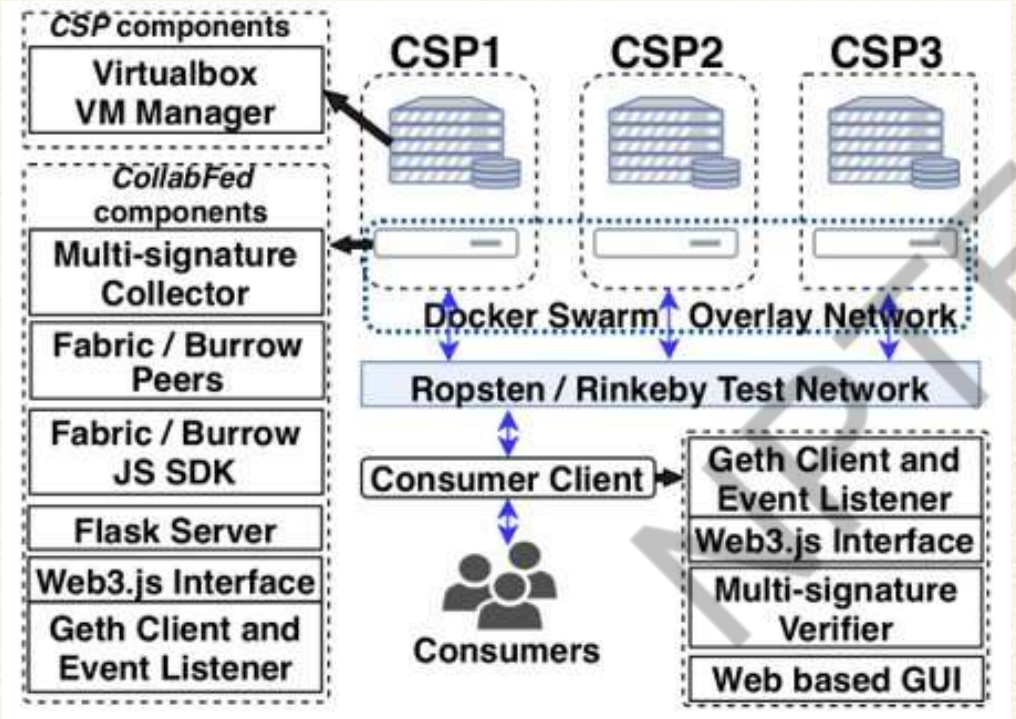
- Consortium of **cloud service providers** (CSPs).
- Provide cloud infrastructure resources to end-users (IaaS).
- Implemented a **fair scheduling algorithm** for allocation of consumer requests among SPs:
    - Each SP will be allocated the number of consumer requests proportional to its infrastructure contribution in the federation.
- Test bed implementation using **Ethereum** and Hyperledger **Fabric**, and Hyperledger **Burrow**.
- Mininet emulation for evaluating scalability.

Use Case Implementation: Cloud Federation

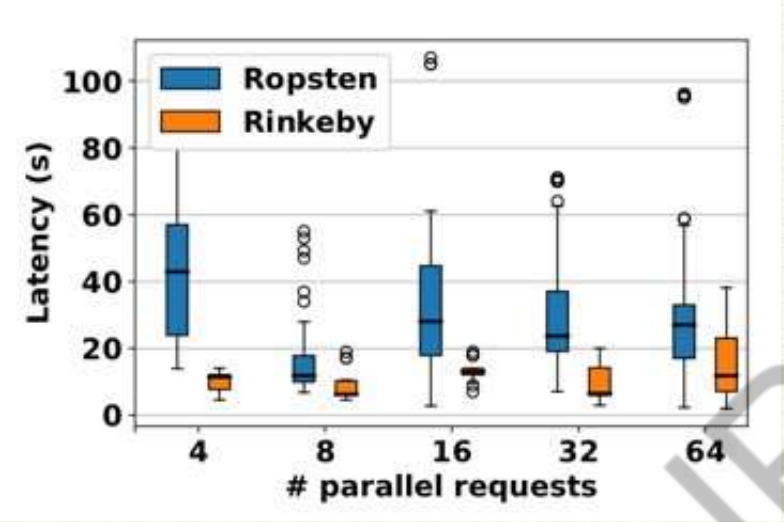


Testbed Setup

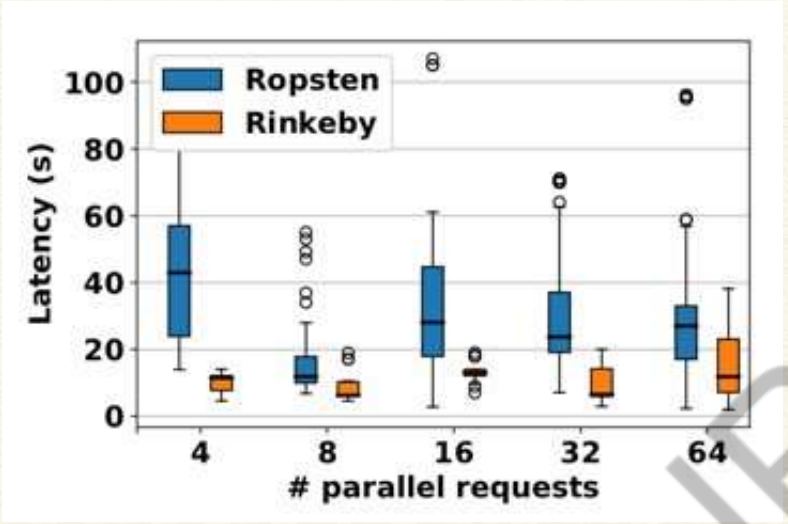
Avg network latency between each server	0.28 ms		
Server configurations	CPU	Memory	OS
CollabCloud server	4 Cores (Intel Core i5-4590 @ 3.30GHz)	8GB	Ubuntu 18.04 (Linux 4.15)
CSP server	88 Cores (Intel Xeon Gold 6152 @ 2.10GHz)	256GB	CentOS 7.7 (Linux 3.10)

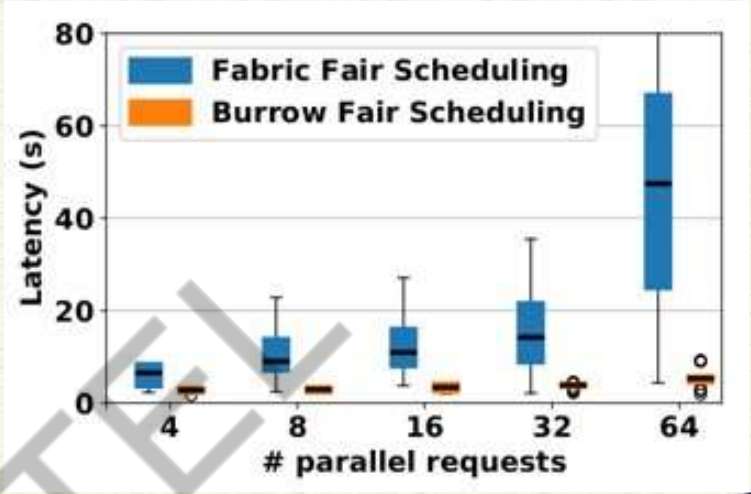


Results

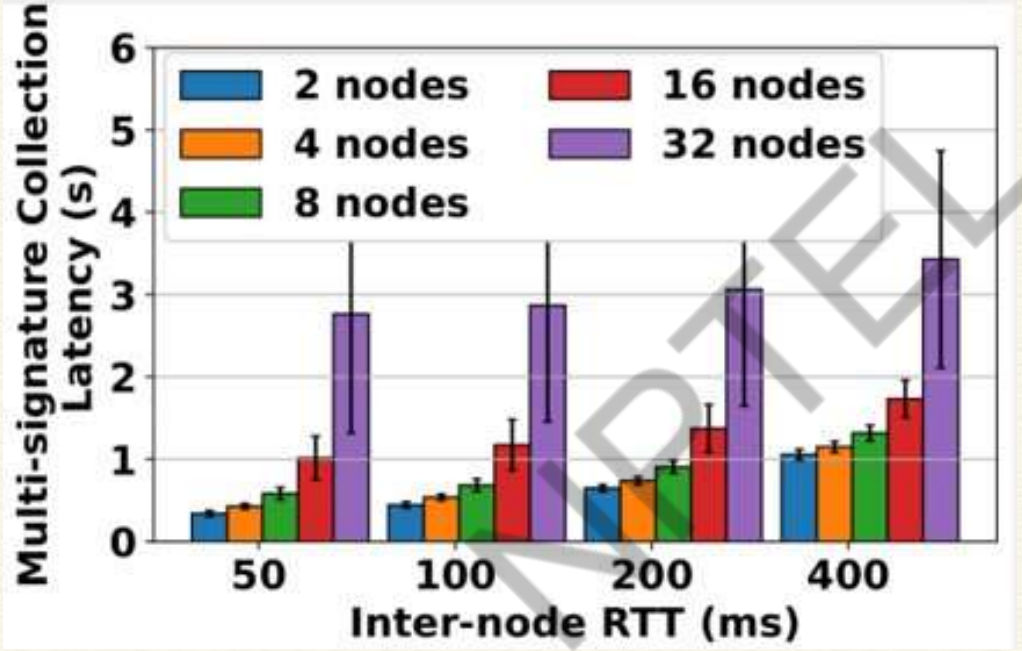


Results





Results



Conclusion

- There are interesting research/design problems in the blockchain space
  - You need to think of applying the right technology at the right place!

- Remember the fundamental questions that we talked about earlier
  - Network, participants, assets, transactions
  - Keys – how to obtain and share
  - Trusted third party – do we have any?
  - Why people will join your blockchain network