

# Blockchain Technology

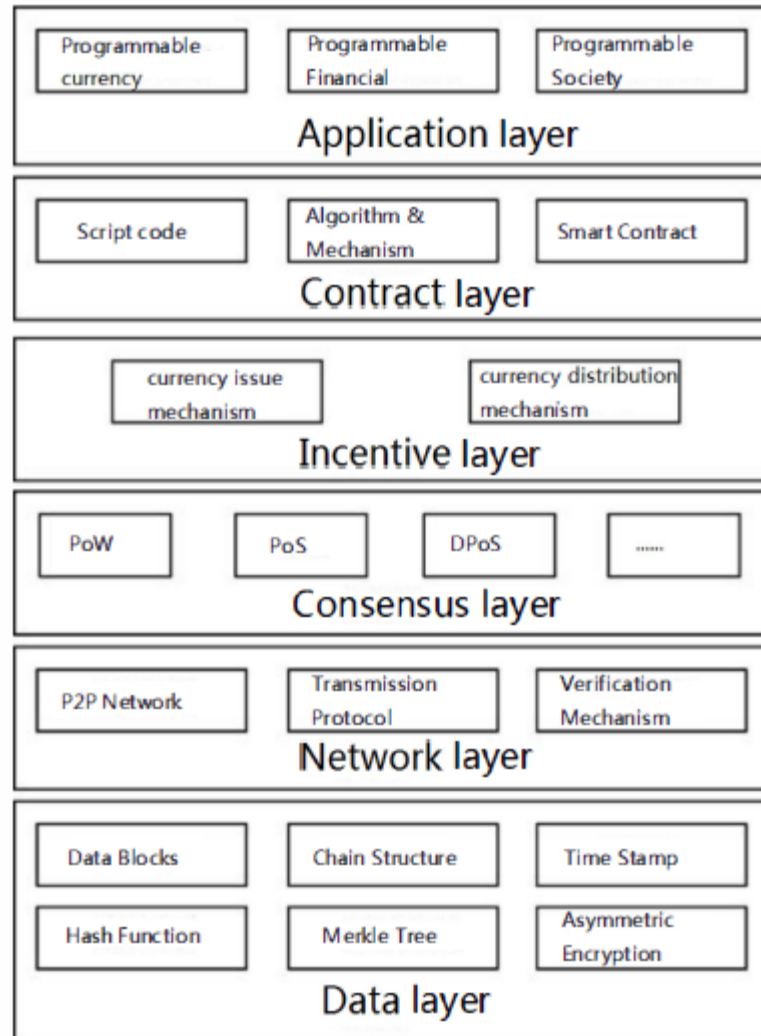
## Research Directions

# Blockchain Technology

## Behind the success of Bitcoin

<b>IoT</b>	<b>Supply Chain</b>	<b>EHR</b>	<b>Copyright Protection</b>	<b>KYC</b>	<b>Land Registry</b>
<b>Data Sharing</b>	<b>Cryptocurrency</b>	<b>Smart Grid</b>	<b>Insurance</b>	<b>Smart Agriculture</b>	<b>Smart Homes</b>
<b>E-Commerce</b>	<b>E-Governance</b>	<b>Social Networking</b>	<b>Education Certificate</b>	<b>File Sharing</b>	<b>Crowd Funding</b>
<b>Postal System</b>	<b>E-Voting</b>	<b>Data Provenance</b>	<b>E-Governance</b>	<b>Asset Transfer</b>	<b>Criminal Record Sharing</b>
		<b>Finance</b>	<b>Many More....</b>		

# Layered Architecture



# Blockchain-based Supply Chain Traceability: Token Recipes model Manufacturing Processes

Martin Westerkamp, Friedhelm Victor and Axel Küpper

Service-centric Networking

Telekom Innovation Laboratories, Technische Universität Berlin

Berlin, Germany

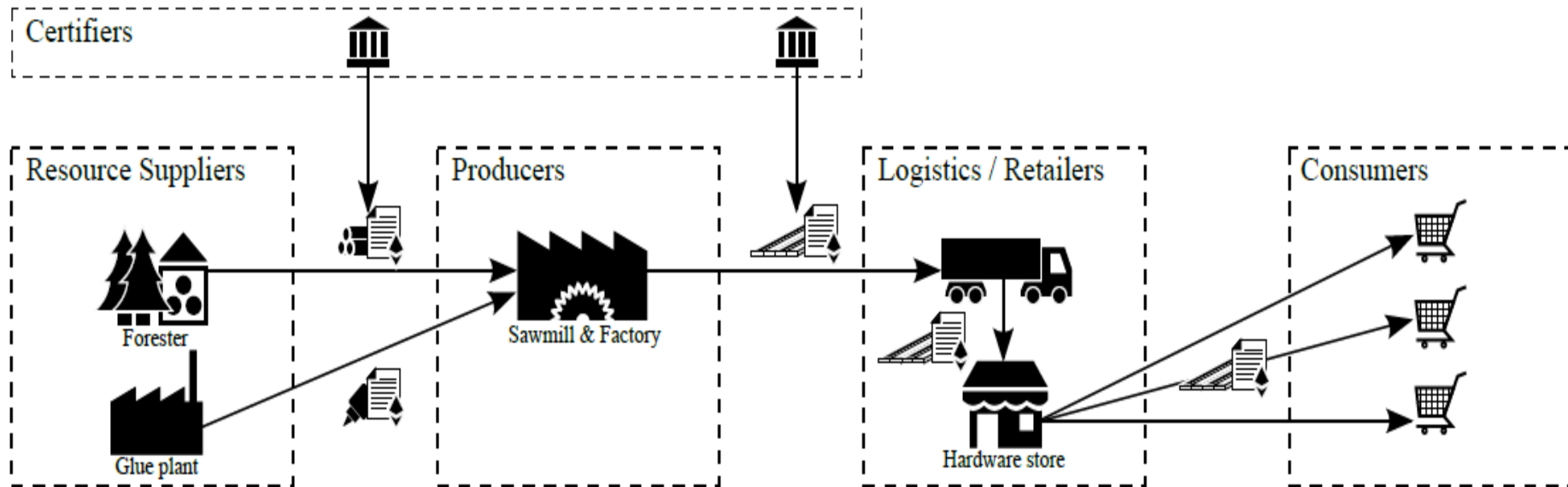
{westerkamp, friedhelm.victor, axel.kuepper}@tu-berlin.de

*Abstract*—Growing consumer awareness as well as manufacturers' internal quality requirements lead to novel demands on supply chain traceability. Existing centralized solutions suffer from isolated data storage and lacking trust when multiple

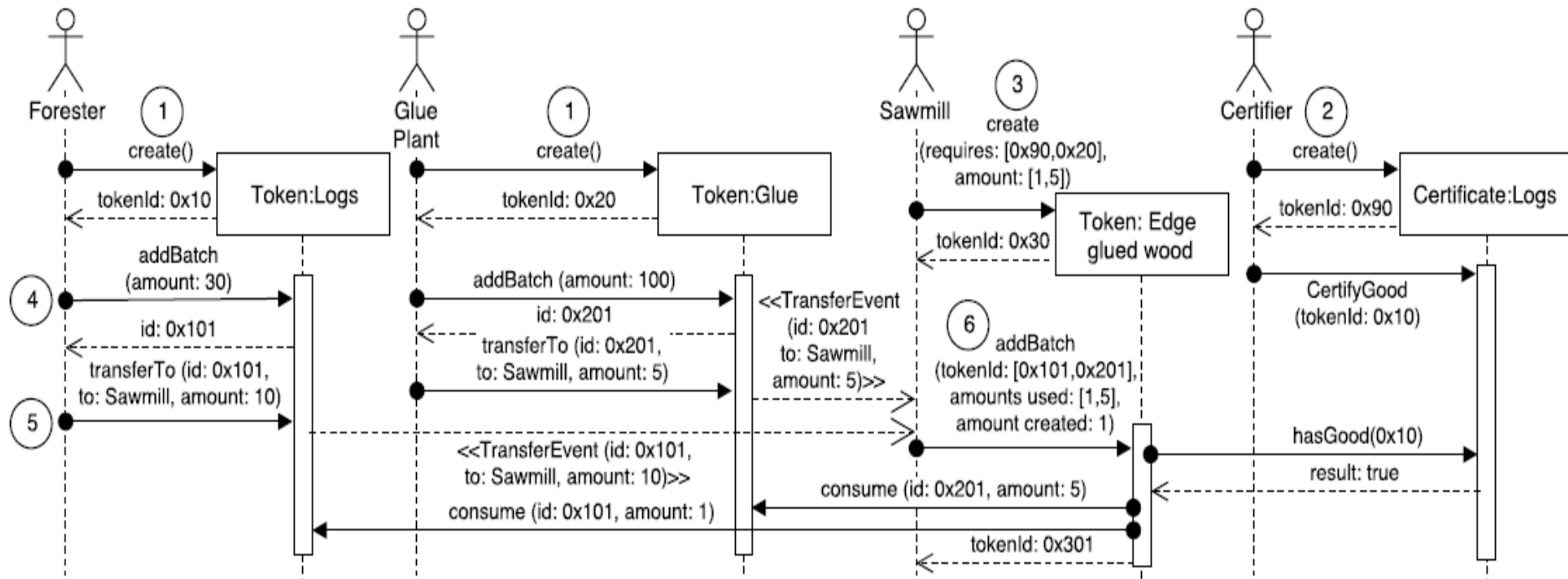
isolated data storage and unsatisfactory standardization in communication and data formats [5], [6].

Recently, blockchain technology has been proposed for providing enhanced traceability in supply chains [6], [7], [8].

# Supply Chain



# Use Case of Supply Chain



# Blockchain for IoT Security and Privacy: The Case Study of a Smart Home

Ali Dorri\*, Salil S. Kanhere \*, Raja Jurdak<sup>†</sup> and Praveen Gauravaram<sup>‡</sup>

\*School of Computer Science and Engineering

The University of New South Wales

Sydney, Australia

Email: (ali.dorri, salil.kanhere)@unsw.edu.au

<sup>†</sup>CSIRO

Brisbane, Queensland, Australia.

Email: Raja.Jurdak@csiro.au

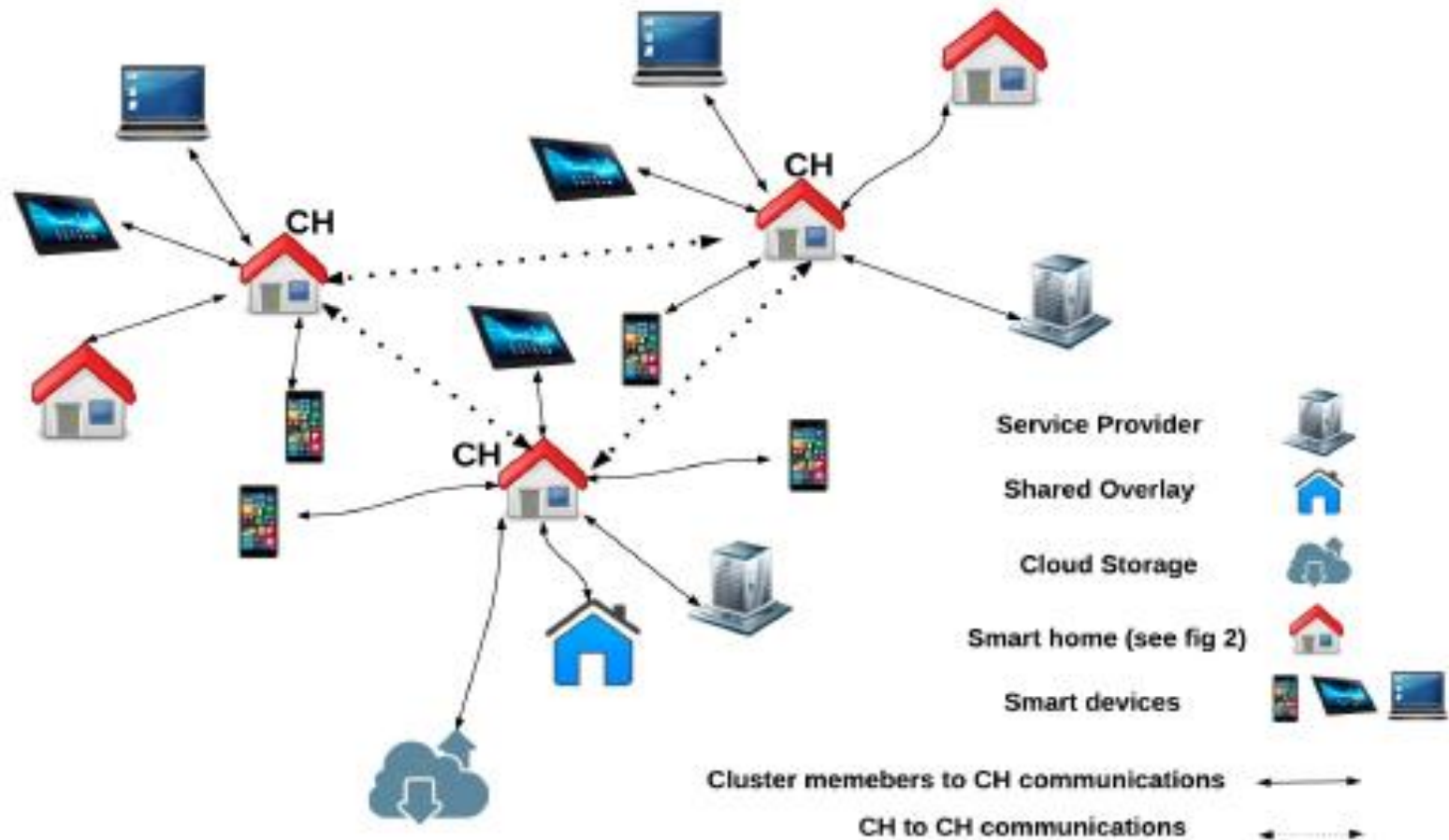
<sup>‡</sup> Tata Consultancy Services, Australia.

Email: p.gauravaram@tcs.com

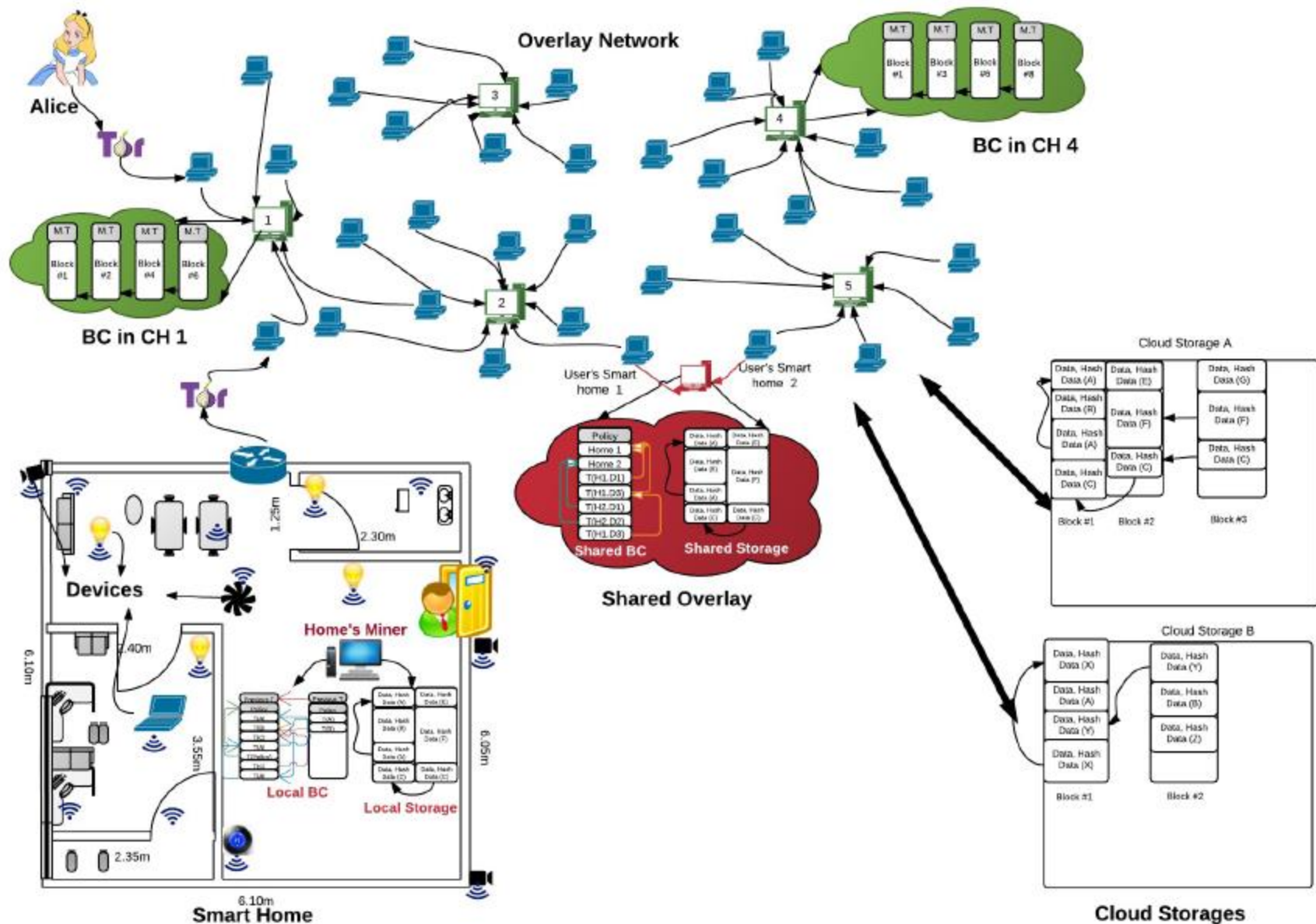
**Abstract**—Internet of Things (IoT) security and privacy remain a major challenge, mainly due to the massive scale and distributed nature of IoT networks. Blockchain-based approaches provide decentralized security and privacy, yet they involve significant energy, delay, and computational overhead that is not suitable for most resource-constrained IoT devices. In our previous work, we presented a lightweight instantiation of a BC particularly geared for use in IoT by eliminating the Proof

hinder some IoT applications from offering personalised services [3]. Consequently, IoT demands a lightweight, scalable, and distributed security and privacy safeguard. The Blockchain (BC) technology that underpins Bitcoin the first cryptocurrency system [4], has the potential to overcome aforementioned challenges as a result of its distributed, secure, and private nature.

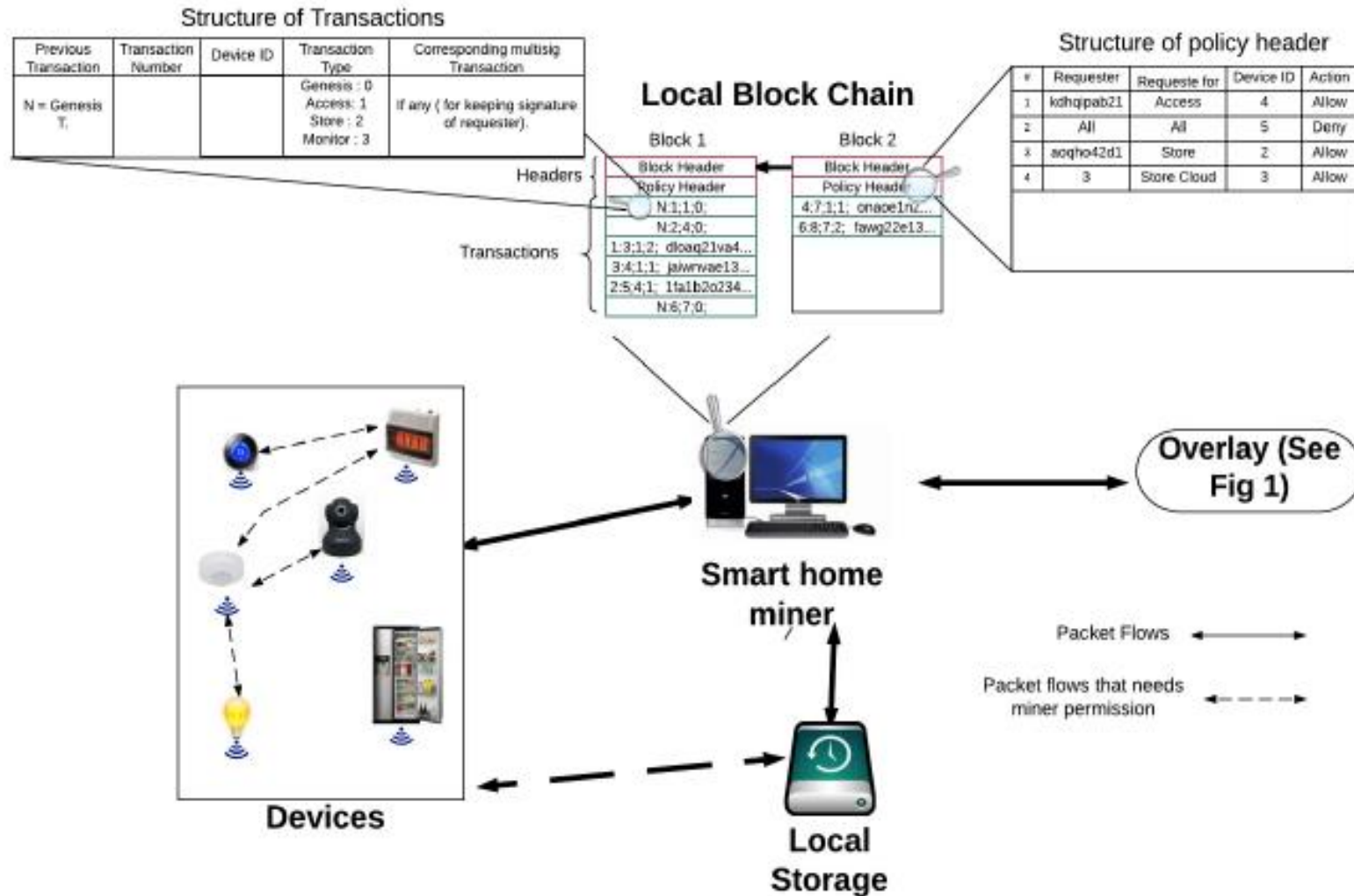
# Smart Homes





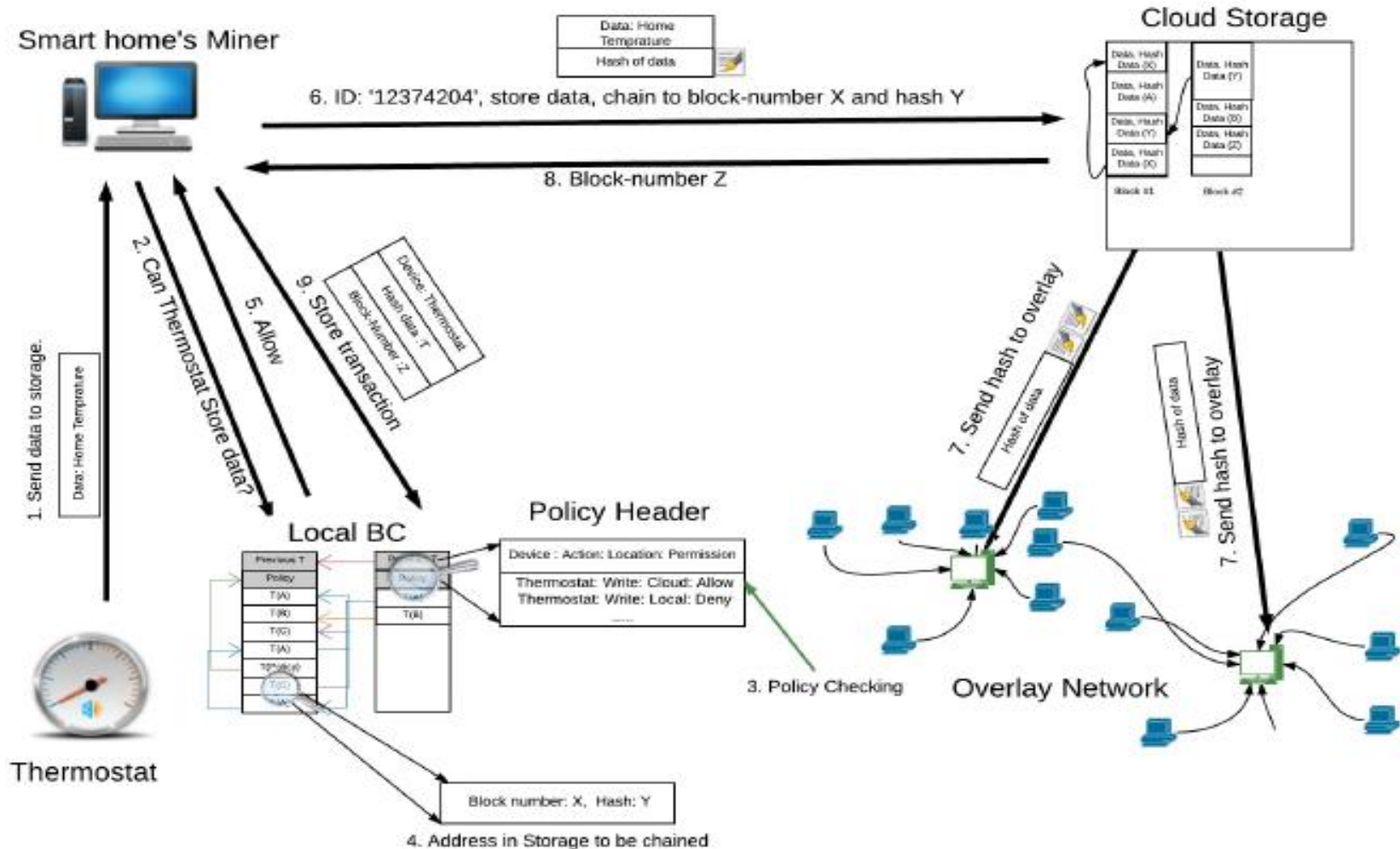


# Smart Homes



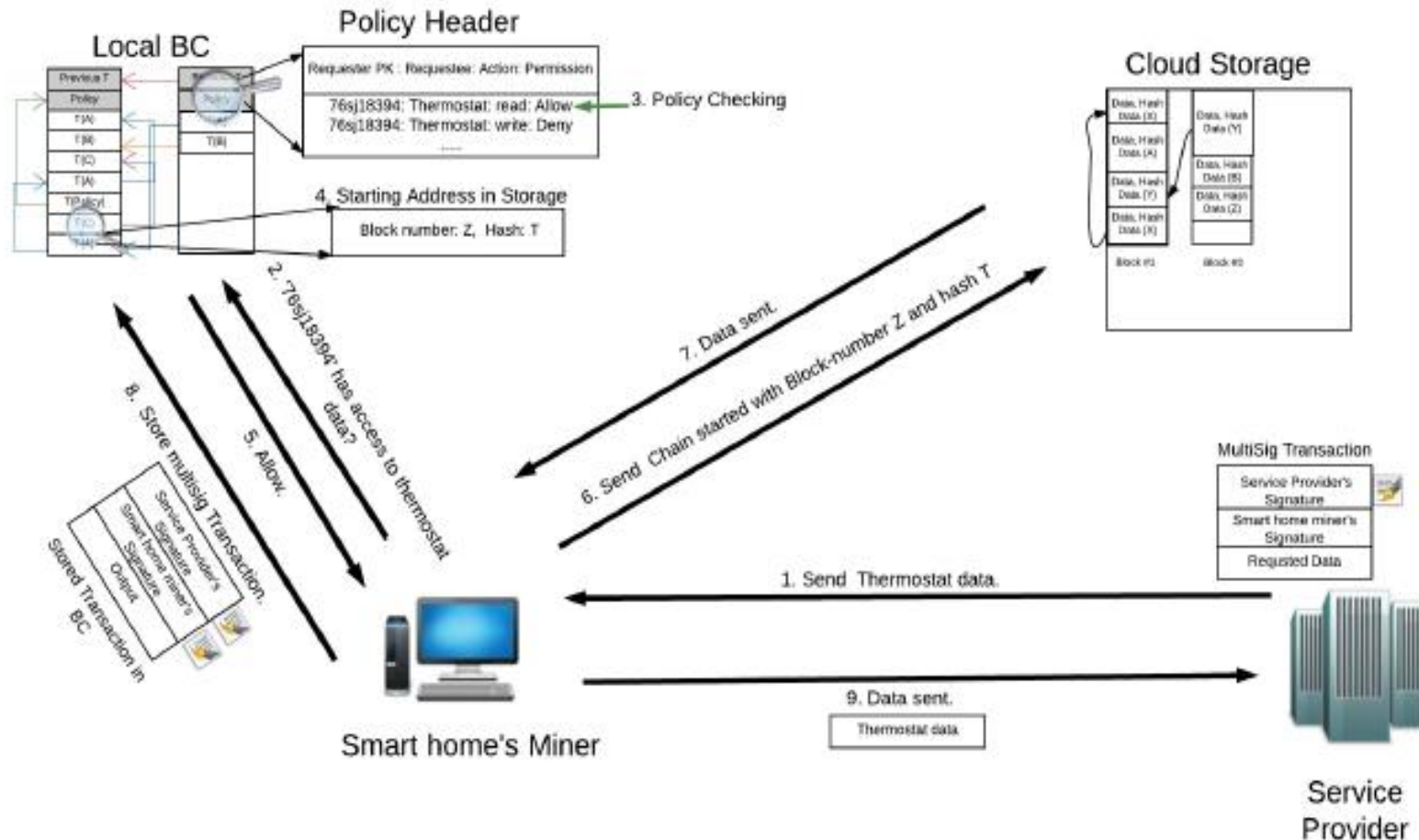
# Smart Homes

## Store Transaction



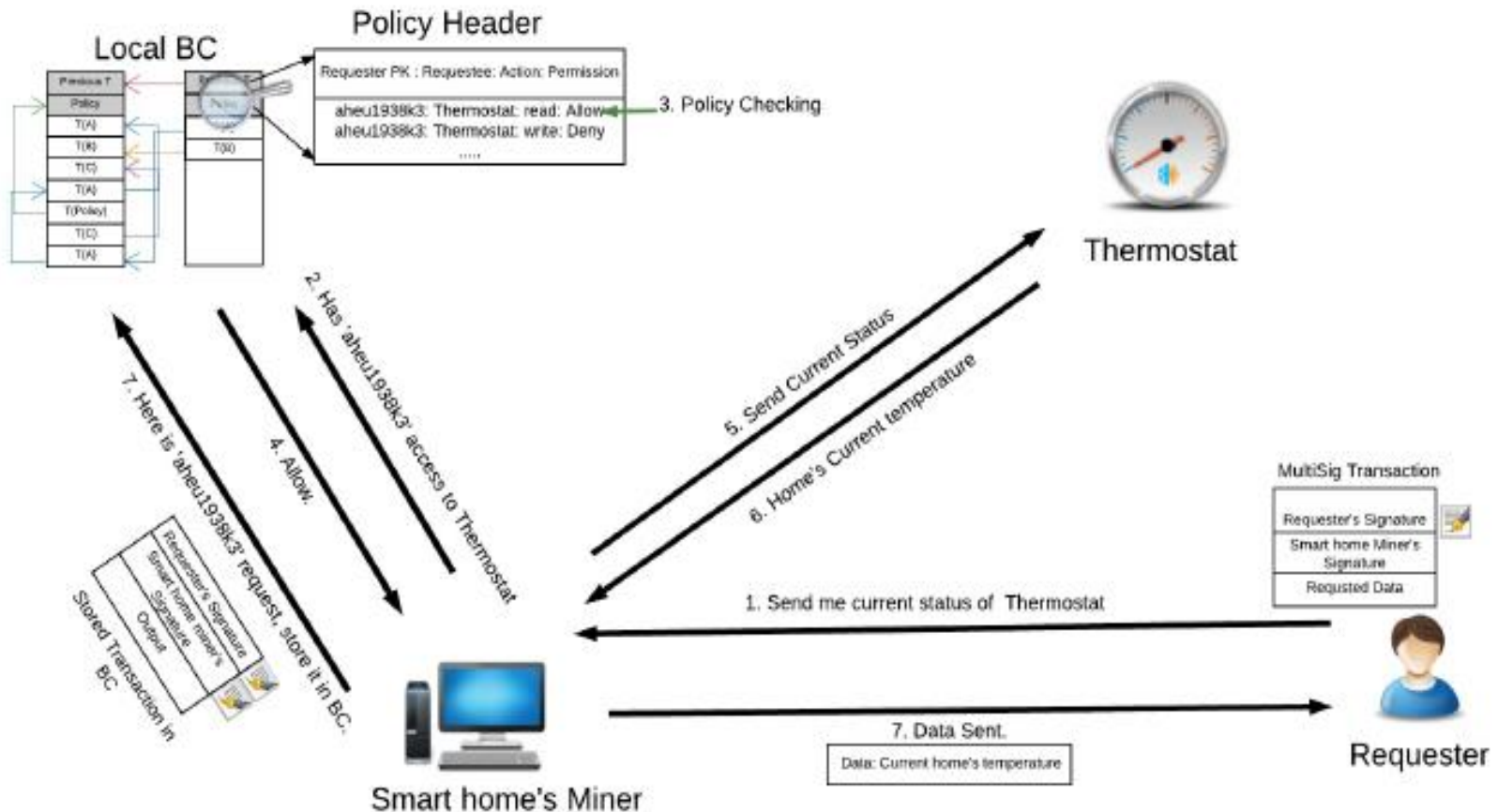
# Smart Homes

## Access Transaction



# Smart Homes

## Monitor Transaction





## Blockchain-based Trusted Computing in Social Network

Dongqi Fu

International School

Beijing University of Posts and Telecommunications

Beijing, China

e-mail: fudongqi@bupt.edu.cn

Liri Fang

School of Environment and Natural Resources

Renmin University of China

Beijing, China

e-mail: fangliri@ruc.edu.cn

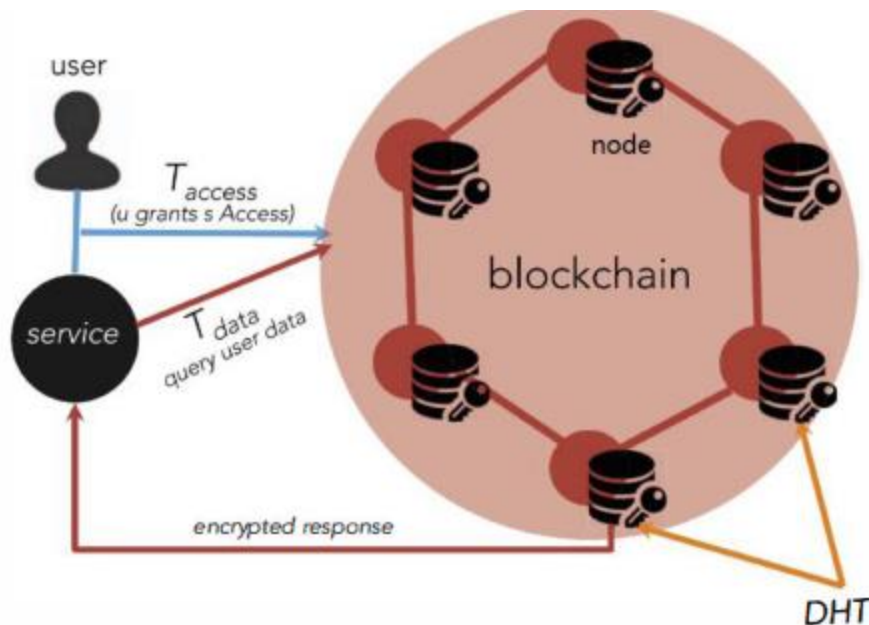
*Abstract*—MIT Media Lab employed blockchain to describe a decentralized personal data management system (i.e. Decentralizing Privacy) that ensures users own and control their data without authentication from a third party. In this paper, we employ a better encryption algorithm from NTT Service Evolution Laboratory to enforce the “Decentralizing

Today, data is a valuable asset in our economy [7]. Facebook, the largest online social-network, collected 300 petabytes of personal data since its inception – a hundred times the amount the Library of Congress has collected in over 200 years [8].

In recent years, a new class of accountable systems

# Data Privacy Management (at MIT)

- Discrete Hash Table (Inter Planetary File System, IPFS)
- Two Transactions:  $T_{access}$  and  $T_{data}$



As illustrated in Fig. 2, the three entities consisting the system are mobile phone users, interested in downloading and using applications; services, the providers of such applications who require processing personal data for operational and business related reasons; and nodes, entities entrusted with maintaining the blockchain and a distributed private key-value data store in return for incentives. The blockchain accepts two new types of transactions:  $T_{access}$ , used for access control management; and  $T_{data}$ , for data storage and retrieval.

# Blockchain-Based E-Voting System

Friðrik Þ. Hjálmarsson, Gunnlaugur K. Hreiðarsson

School of Computer Science

Reykjavik University, Iceland

{fridrik14, gunnlaugur15}@ru.is

*Abstract*—Building an electronic voting system that satisfies the legal requirements of legislators has been a challenge for a long time. Distributed ledger technologies is an exciting technological advancement in the information technology world. Blockchain technologies offer an infinite range of applications benefiting from sharing economies. This paper aims to evaluate the application of blockchain as service to implement distributed electronic

(iv) A majority of the network nodes must reach a consensus before a proposed new block of entries becomes a permanent part of the ledger.

These technological features operate through advanced cryptography, providing a security level equal and/or greater



# Election as Smart Contract

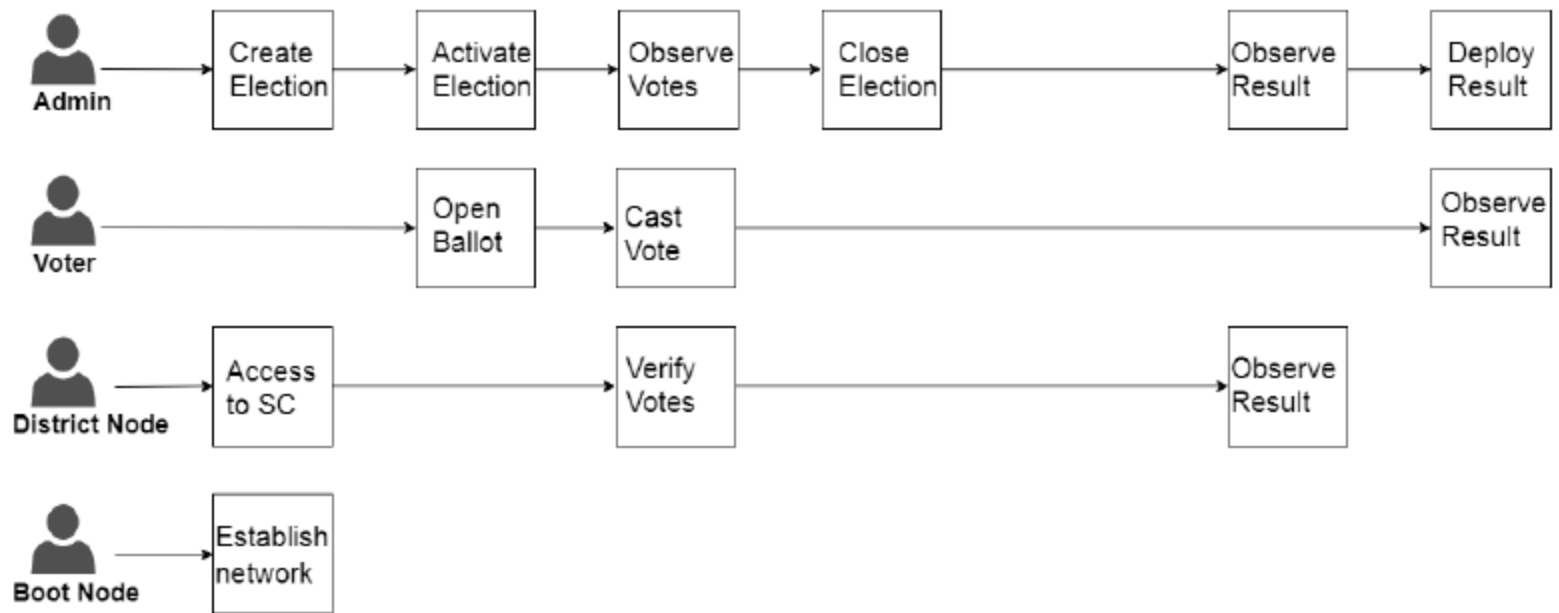
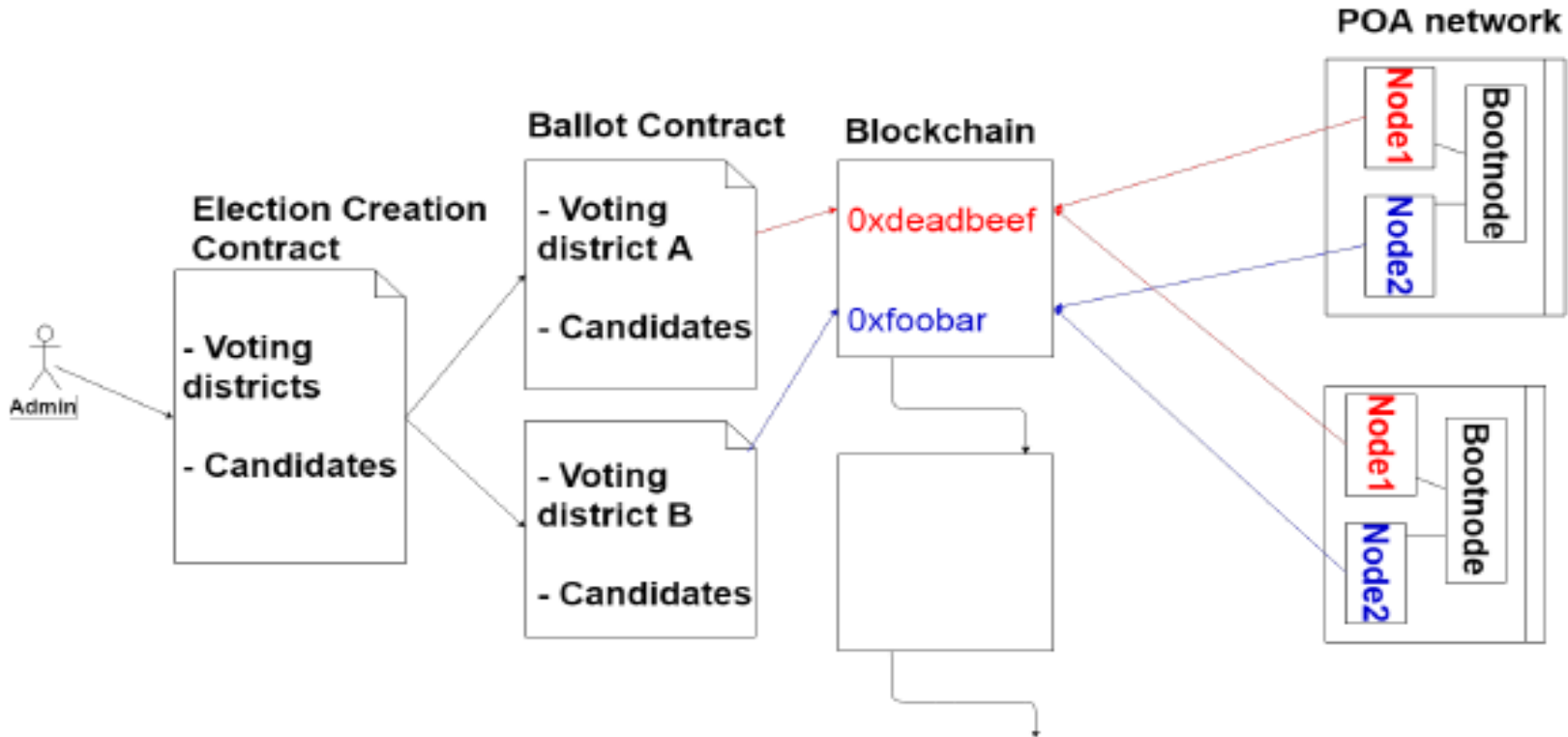


Fig. 1: Election roles and process

# Election as Smart Contract



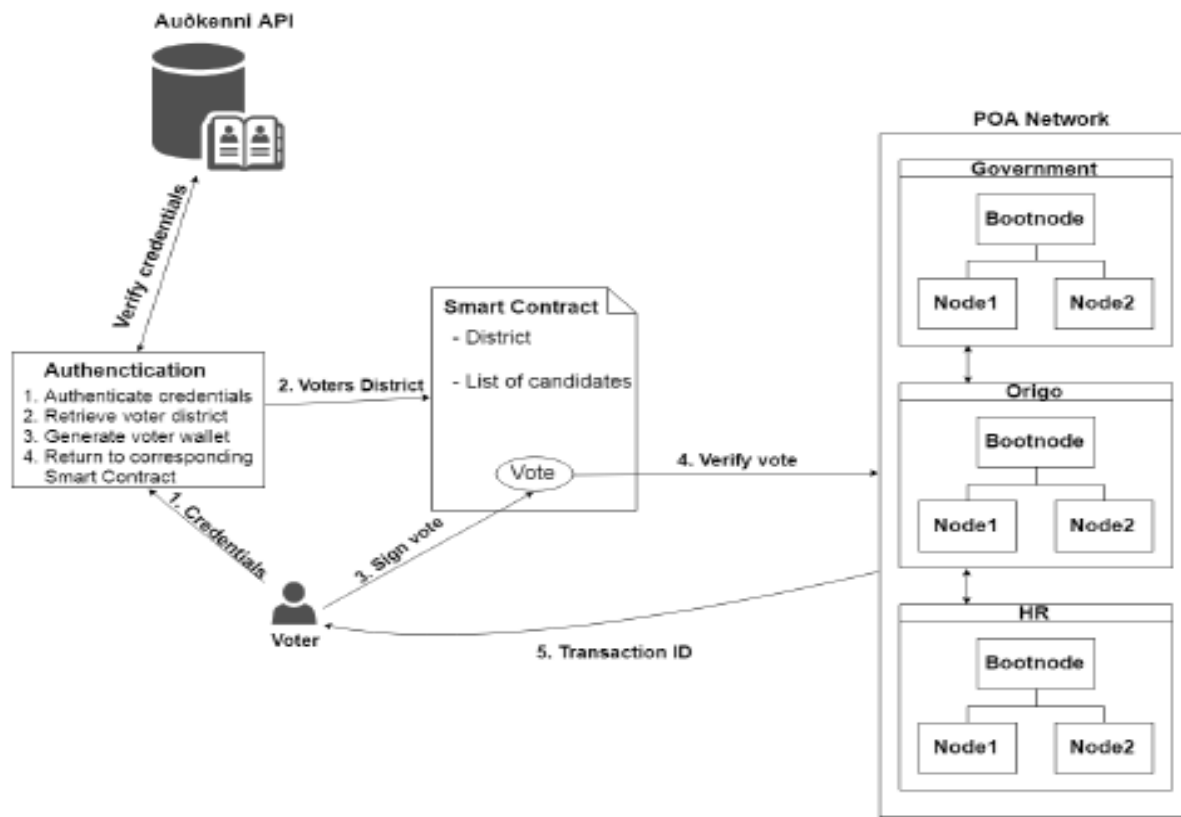


Fig. 3: Voter authenticates himself and casts vote

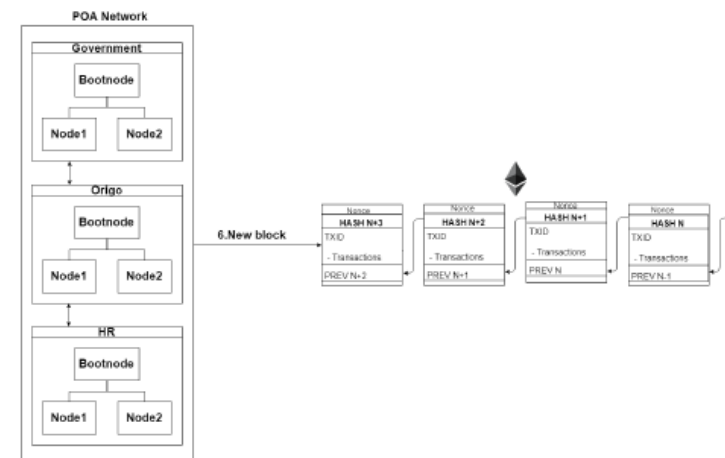


Fig. 4: Block added to the blockchain

# Blockchain for Secure EHRs Sharing of Mobile Cloud Based E-Health Systems

DINH C. NGUYEN<sup>1</sup>, PUBUDU N. PATHIRANA<sup>1</sup>, (Senior Member, IEEE),  
MING DING<sup>2</sup>, (Senior Member, IEEE), AND  
ARUNA SENEVIRATNE<sup>3</sup>, (Senior Member, IEEE)

<sup>1</sup>School of Engineering, Deakin University, Waurn Ponds, VIC 3216, Australia

<sup>2</sup>Data61, CSIRO, Kensington, WA 6152, Australia

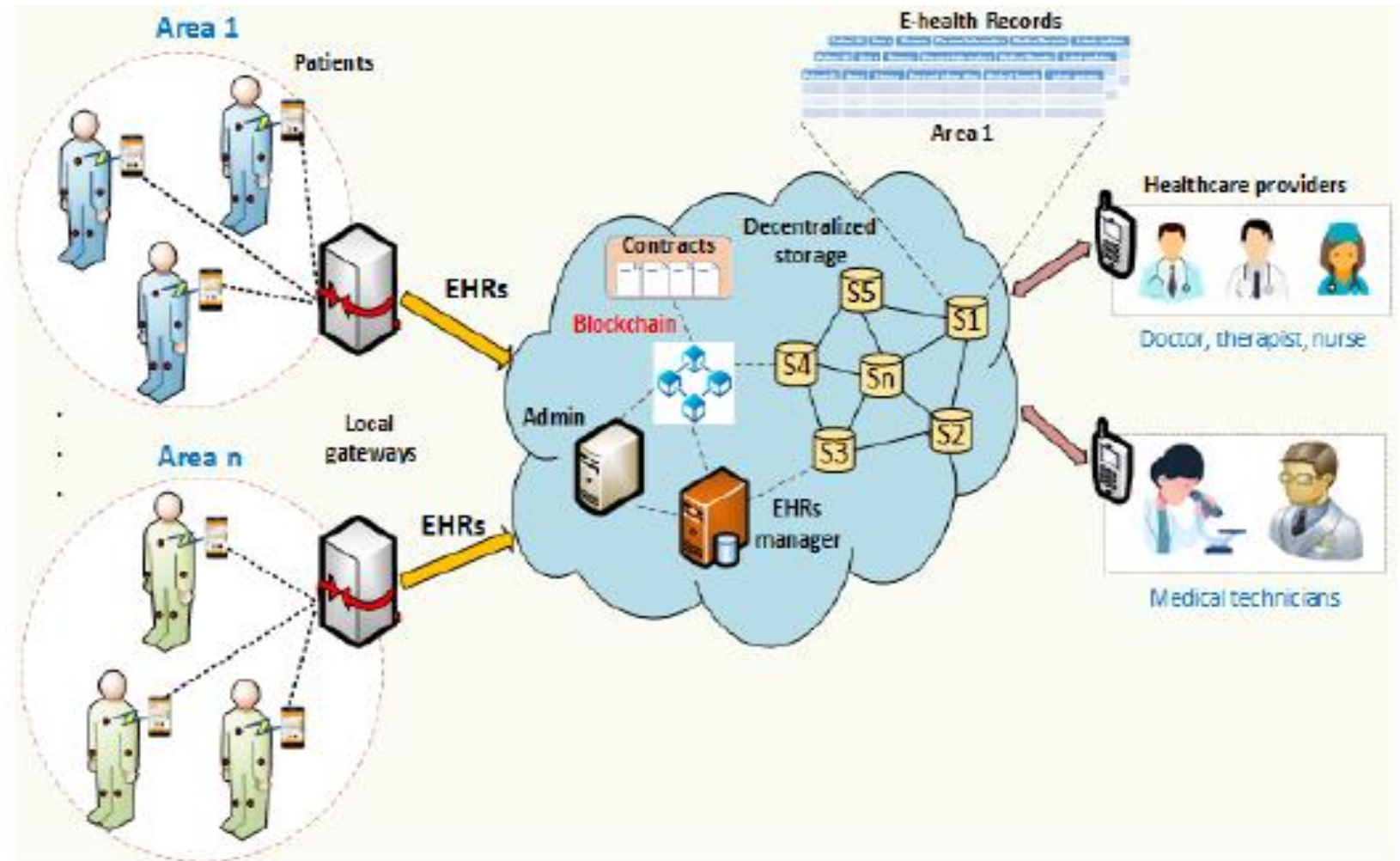
<sup>3</sup>School of Electrical Engineering and Telecommunications, University of New South Wales (UNSW), Sydney, NSW 2052, Australia

Corresponding author: Dinh C. Nguyen (cdnguyen@deakin.edu.au)

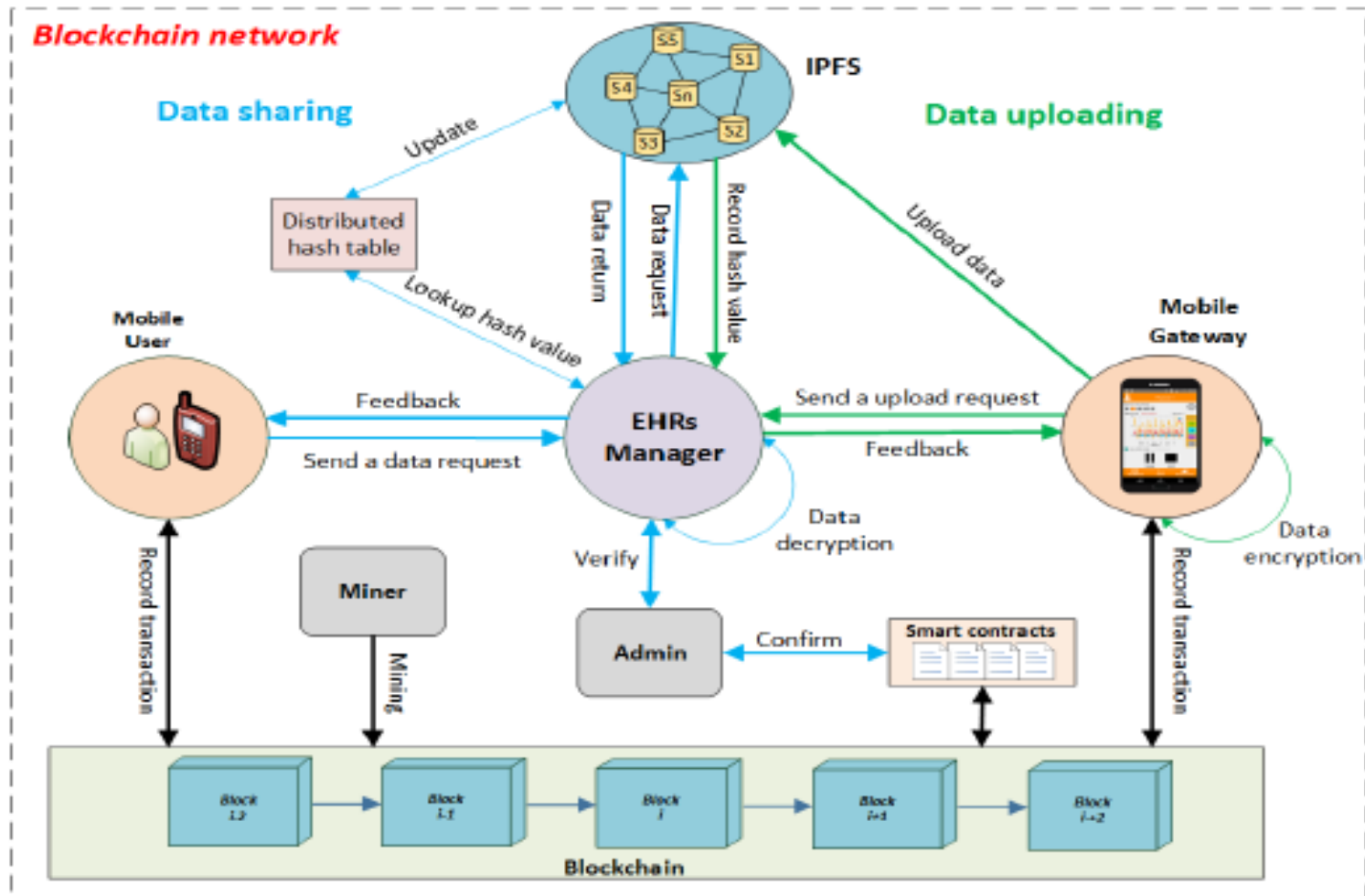
This work was supported in part by the CSIRO Data61, Australia.

⋮ **ABSTRACT** Recent years have witnessed a paradigm shift in the storage of Electronic Health Records (EHRs) on mobile cloud environments, where mobile devices are integrated with cloud computing to facilitate medical data exchanges among patients and healthcare providers. This advanced model enables healthcare services with low operational cost, high flexibility, and EHRs availability. However, this new paradigm also raises concerns about data privacy and network security for e-health systems. How to reliably share EHRs among mobile users while guaranteeing high-security levels in the mobile cloud is a challenging issue. In this paper, we propose a novel EHRs sharing framework that combines blockchain and the decentralized interplanetary file system (IPFS) on a mobile cloud platform. Particularly, we design a trustworthy access control mechanism using smart contracts to achieve secure EHRs sharing among different

# HealthCare



# HealthCare





DIGITAL SYSTEMS & TECHNOLOGY

---



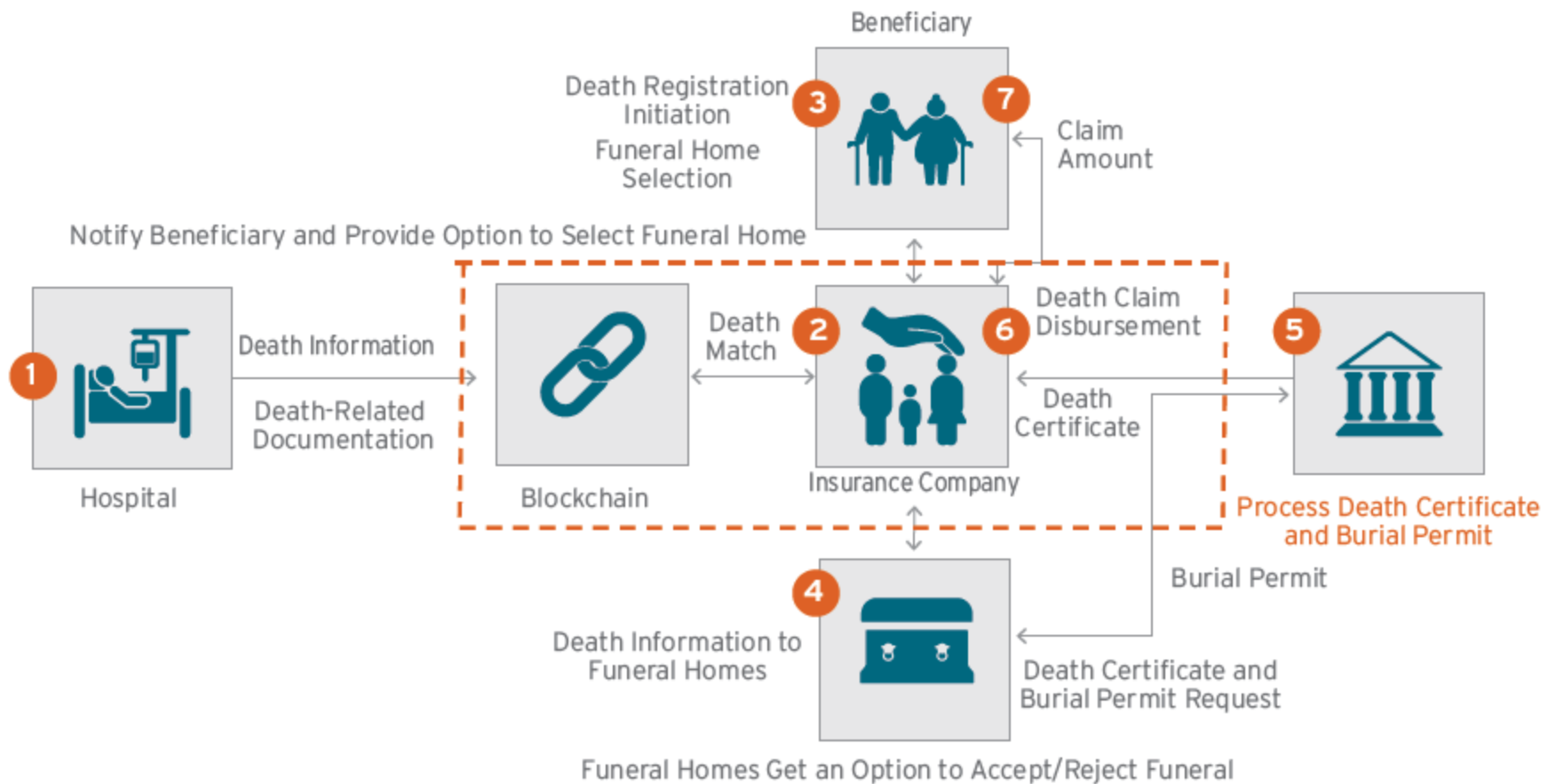
Cognizant

# Blockchain: A Potential Game-Changer for Life Insurance

---

In a world in search of more open, trusted and secure IT systems, all eyes are on blockchain, which through its distributed ledger, smart contracts and non-repudiation capabilities acts as a shared infrastructure that can transform multiple processes across the insurance value chain. Here's how.

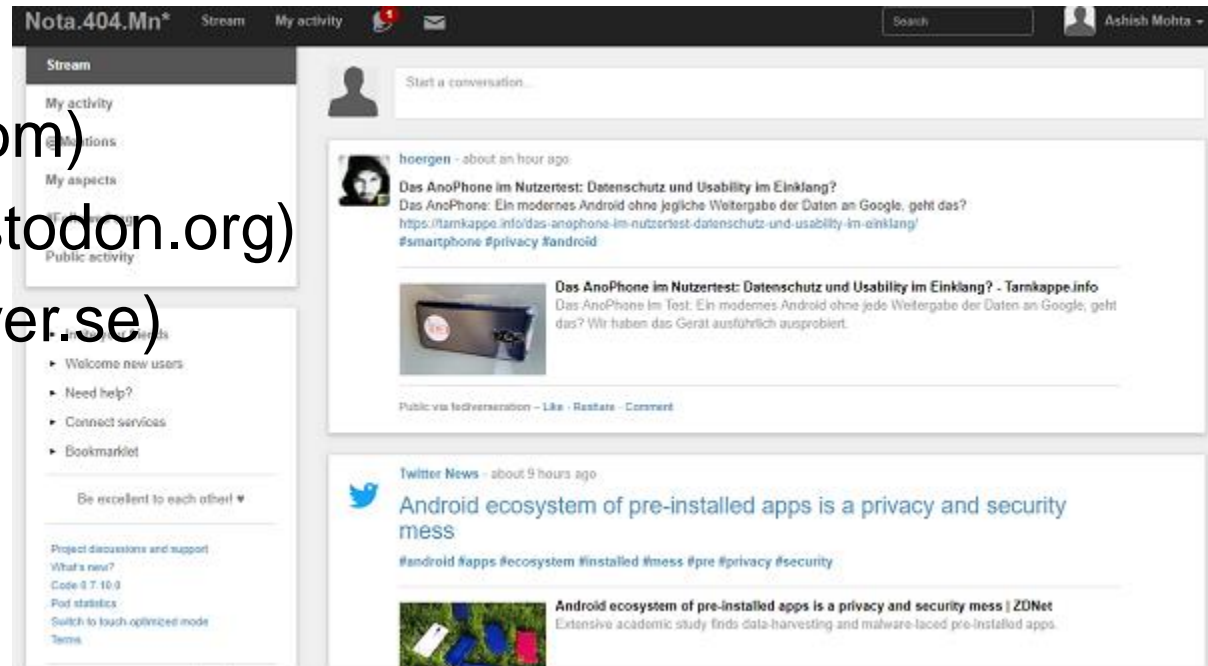
# Claim after death!





# Decentralised Social Network

- 1] Diaspora ([diasporafoundation.org](https://diasporafoundation.org))
- 2] SocialX ([socialx.network](https://socialx.network))
- 3] Minds ([wefunder.com/minds](https://wefunder.com/minds))
- 4] Memo ([memo.cash](https://memo.cash))
- 5] Sola ([sola.ai](https://sola.ai))
- 6] Steemit ([steemit.com](https://steemit.com))
- 7] Mastodon ([joinmastodon.org](https://joinmastodon.org))
- 8] Manyverse ([manyver.se](https://manyver.se))



## **ProvChain: A Blockchain-based Data Provenance Architecture in Cloud Environment with Enhanced Privacy and Availability**

Xueping Liang<sup>1</sup>, Sachin Shetty<sup>2</sup>, Deepak Tosh<sup>3</sup>, Charles Kamhoua<sup>4</sup>, Kevin Kwiat<sup>4</sup>, and Laurent Njilla<sup>4</sup>

<sup>1</sup> College of Engineering, Tennessee State University, Nashville, TN 37209

<sup>2</sup> Virginia Modeling Analysis and Simulation Center, Old Dominion University, Norfolk, VA 23529

<sup>3</sup> Department of Computer Science, Norfolk State University, Norfolk, VA 23504

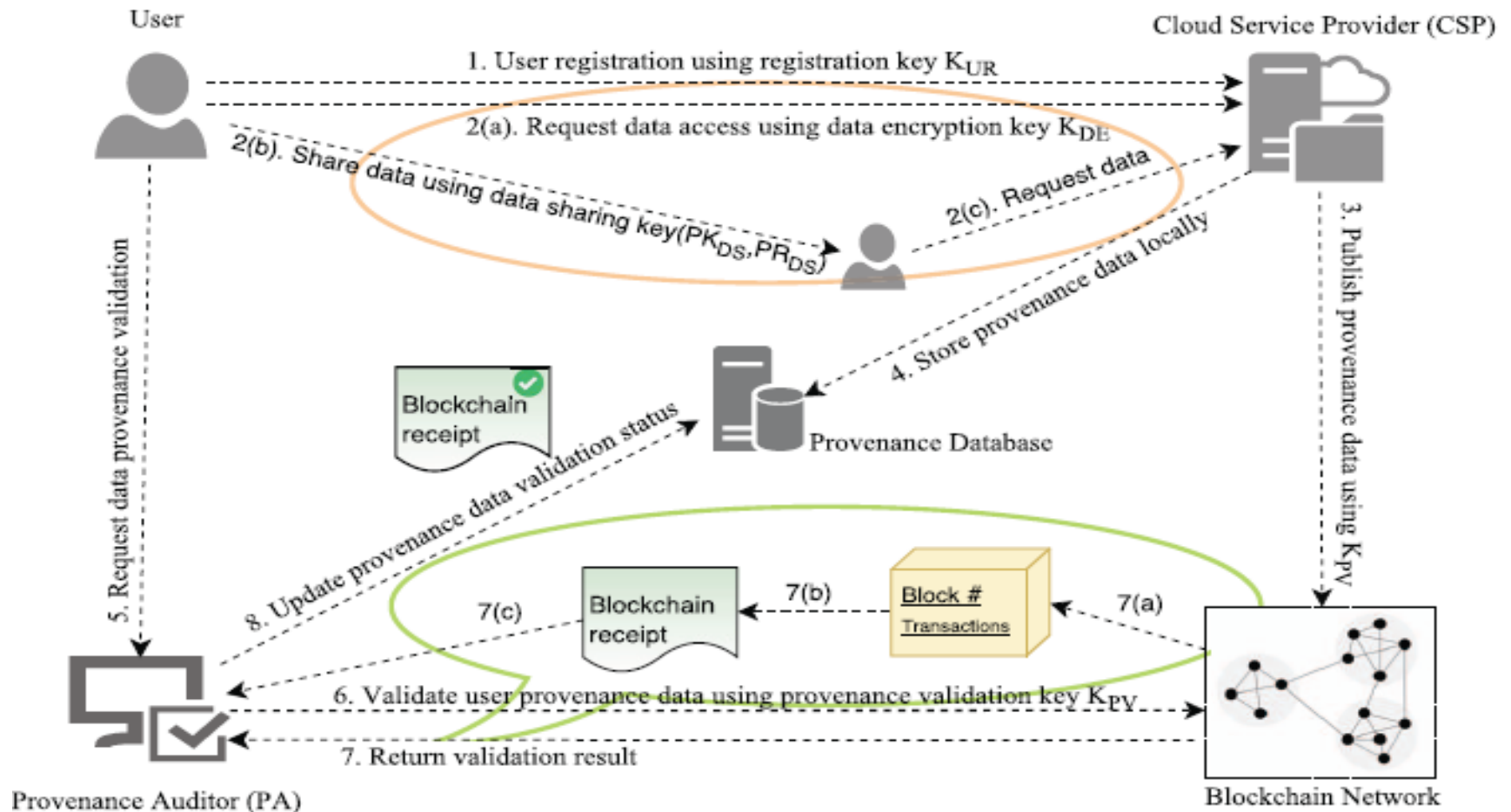
<sup>4</sup> Cyber Assurance Branch, Air Force Research Laboratory, Rome, NY 13441

xliang@tnstate.edu, sshetty@odu.edu, dktosh@nsu.edu,  
{charles.kamhoua.1, kevin.kwiat, laurent.njilla}@us.af.mil

**Abstract**—Cloud data provenance is metadata that records the history of the creation and operations performed on cloud data object. Secure data provenance is crucial for data accountability, forensics and privacy. In this paper, we propose a decentralized and trusted cloud data provenance


provenance remains a critical issue for cloud storage applications. Besides, provenance data may contain sensitive information about the original data and the data owners. Hence, there is a need to secure not only the cloud data

# Blockchain-based Data Provenance in Cloud



Article

# A Hierarchical and Abstraction-Based Blockchain Model

Swagatika Sahoo<sup>1</sup>, Akshay M. Fajge<sup>1</sup>, Raju Halder<sup>1</sup> and Agostino Cortesi<sup>2,\*</sup> 

<sup>1</sup> Department of Computer Science and Engineering, Indian Institute of Technology Patna, Bihta, Patna 801106, Bihar, India; swagatika\_1921cs03@iitp.ac.in (S.S.); fajge\_1921cs12@iitp.ac.in (A.M.F.); halder@iitp.ac.in (R.H.)

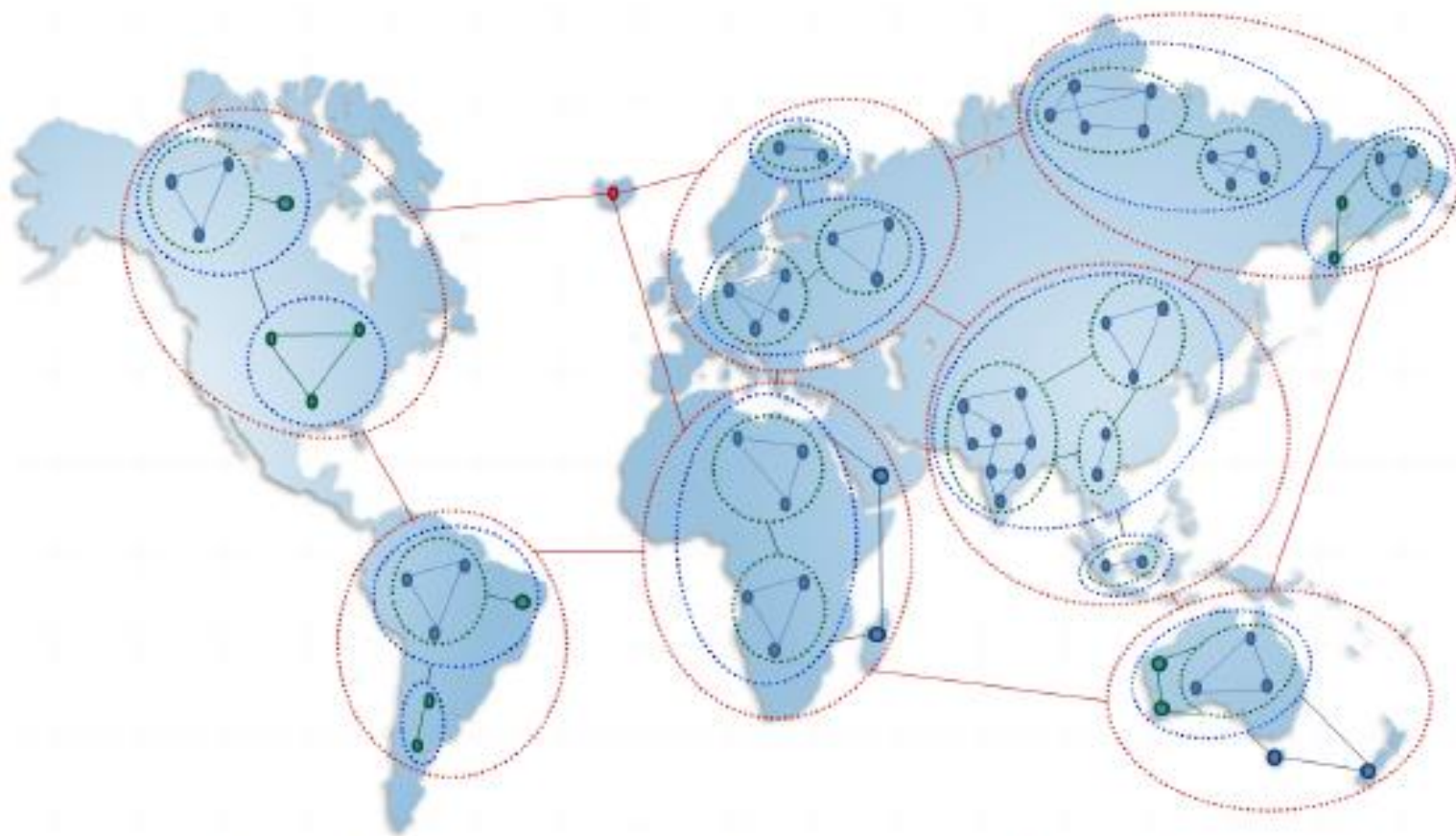
<sup>2</sup> Dipartimento di Scienze Ambientali, Informatica e Statistica, Università Ca' Foscari, via Torino 155, 30170 Venice, Italy

\* Correspondence: cortesi@unive.it

Received: 24 April 2019; Accepted: 5 June 2019; Published: 7 June 2019



**Abstract:** In the nine years since its launch, amid intense research, scalability is always a serious concern in blockchain, especially in case of large-scale network generating huge number of transaction-records. In this paper, we propose a hierarchical blockchain model characterized by: (1) multi-level branching multiple levels of blocks in a tree structure; (2) multi-level blocks in a sequential



**Figure 1.** Decentralized network views at various levels of hierarchy.



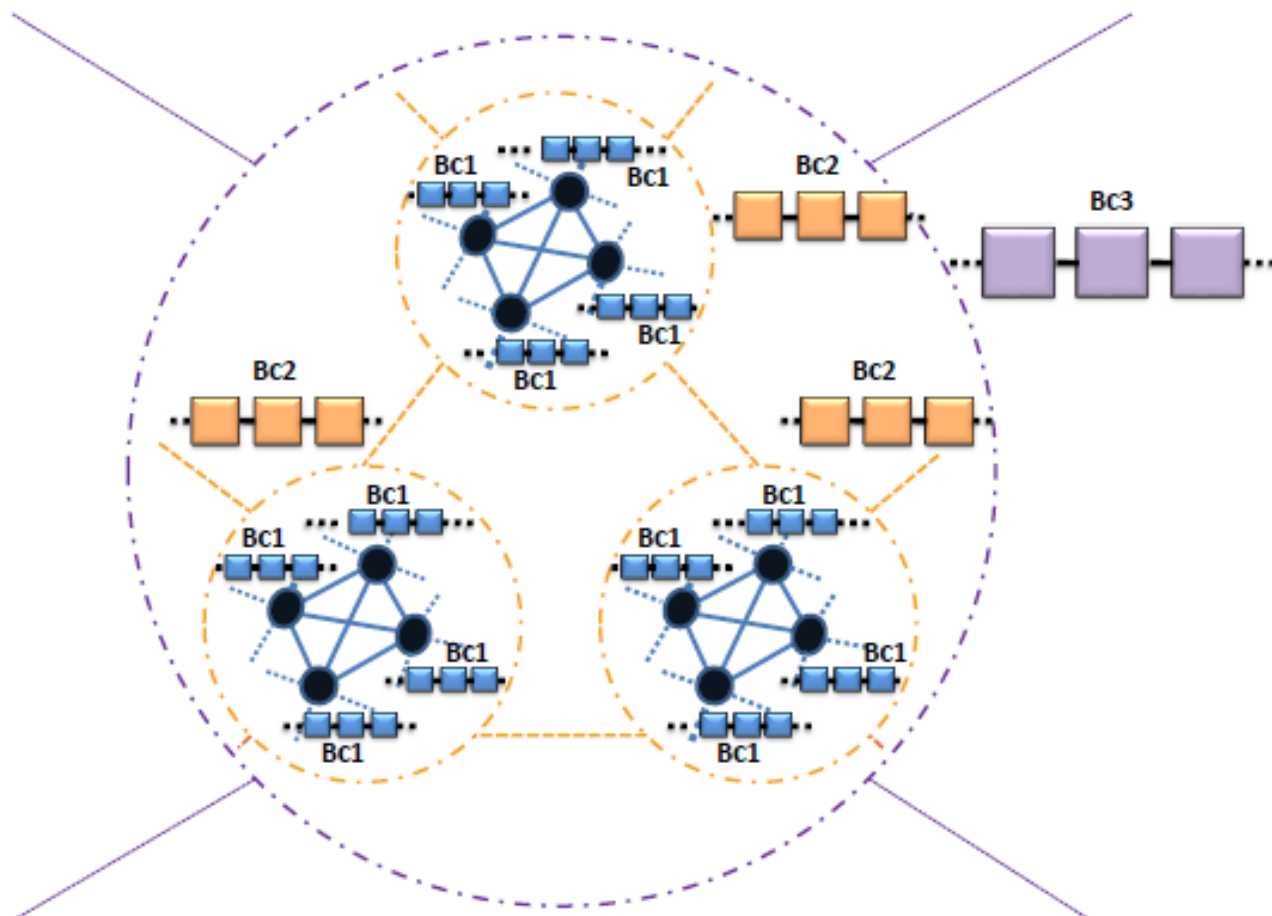


Figure 2. Schematic diagram of hierarchical blockchains model.

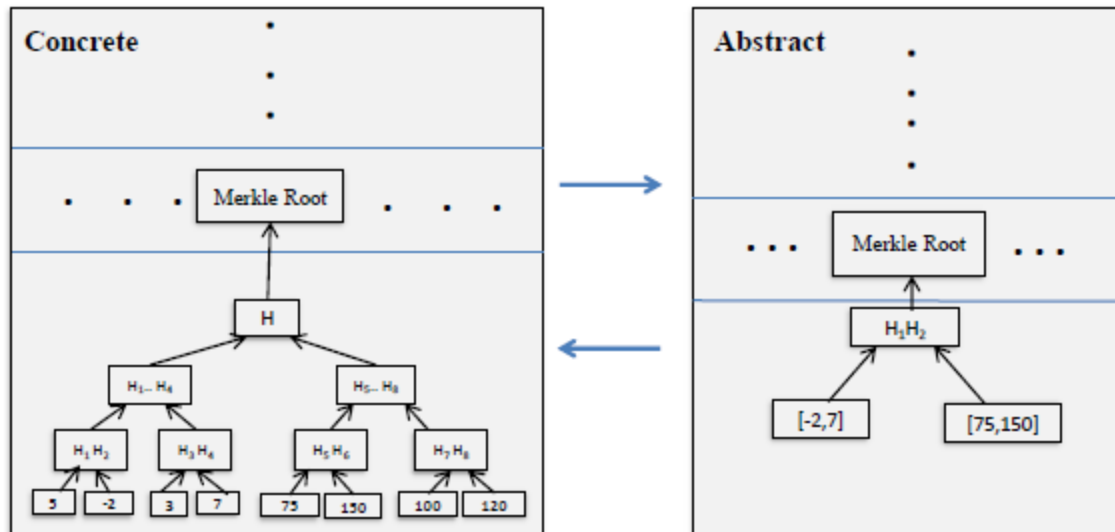


Figure 8. Abstract Block in Interval Domain.

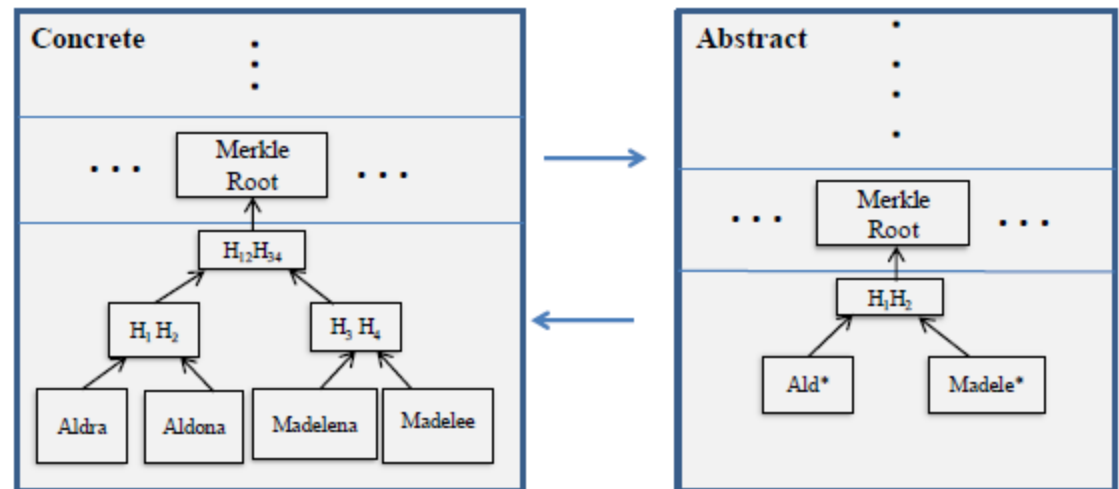


Figure 9. Abstract Block in Prefix Domain.

# BDmark: A Blockchain-driven Approach to Big Data Watermarking

Swagatika Sahoo<sup>1</sup>, Rishu Roshan<sup>2</sup>, Vikash Singh<sup>2</sup>, and Raju Halder<sup>1</sup>

<sup>1</sup> Indian Institute of Technology Patna, India  
{swagatika\_1921cs03,halder}@iitp.ac.in

<sup>2</sup> Indian Institute of Information Technology Guwahati, India  
{rishuroshan.1998, vik625singh}@gmail.com

**Abstract.** Over the last decade, most enterprises are harnessing the power of big data as a driving force to their business growth. This creates a new paradigm which encourages large number of start-ups and less-known data brokers to adopt data monetization as their key role in the data marketplace. As a pitfall, such data-driven scenarios make big data prone to various threats, such as ownership claiming, illegal reselling, tampering, etc. Unfortunately, existing watermarking solutions are ill-suited to big



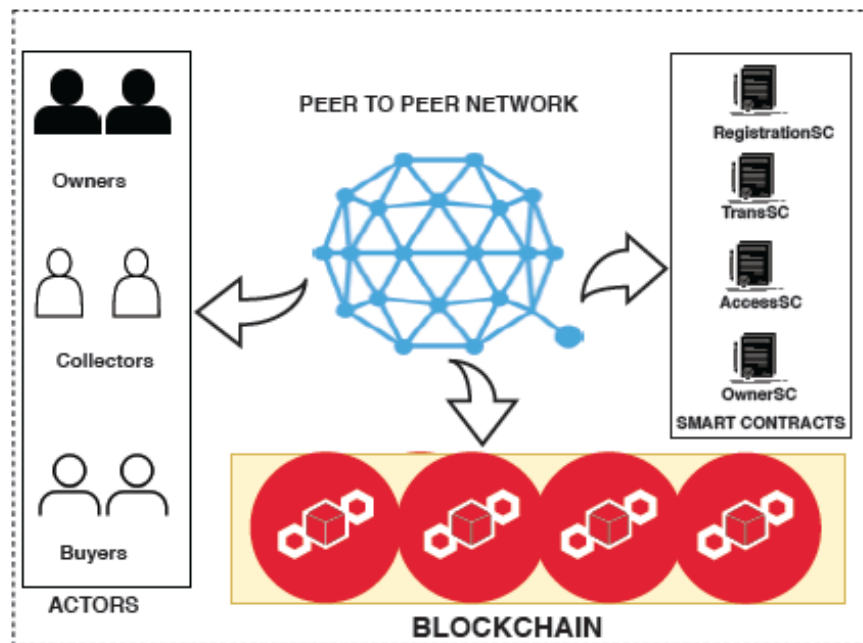


Fig. 1: A pictorial representation of the overall system components

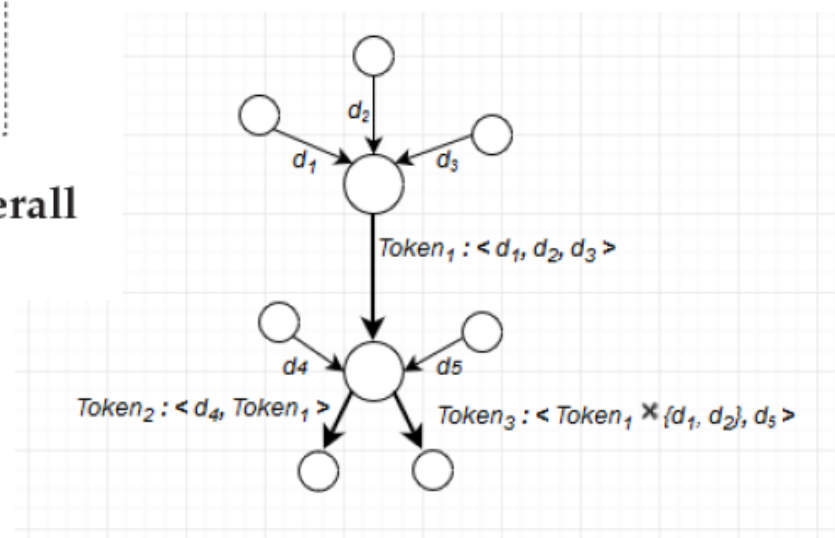


Fig. 4: Data transfer scenarios involving data-collection, aggregation and splitting through token generation

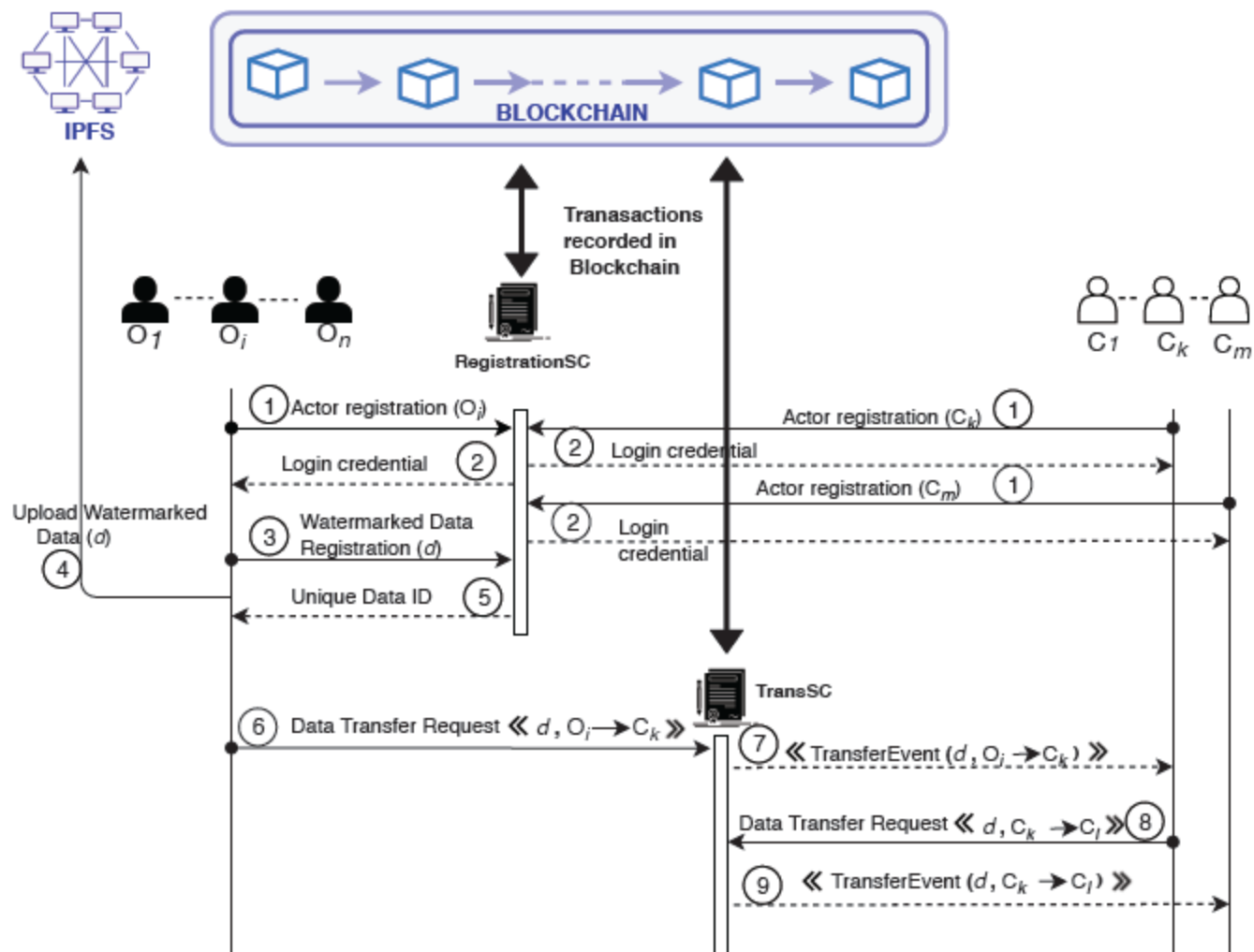


Fig. 2: Interaction-diagram among owners, collectors and smart contracts

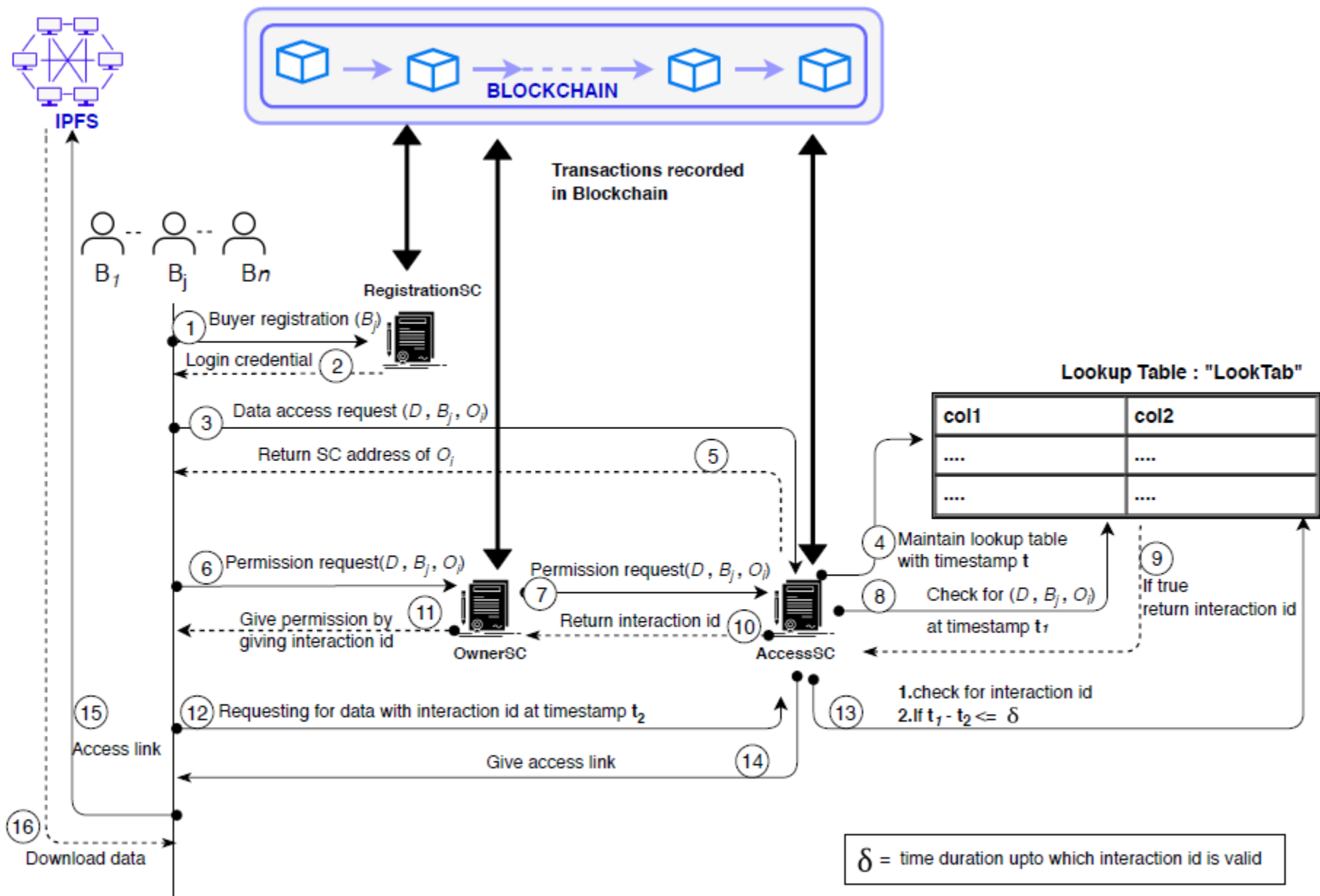


Fig. 3: Interaction-diagram between data-buyers and smart contracts.

# More!

- Asset Transfer
- Smart Agriculture
- Postal Services
- Land Registry
- KYC
- Criminal Records Keeping

Topics (All based on Blockchain)
Blockchain-based File Tracking System using QR code and Android App
Blockchain-based Charitable Donations Tracking System
Meeting Room Booking System (Blockchain + Android App)
Mess Complaint Management System (Blockchain + Android App)
A common blockchain-based Platform for Criminal Records
Bringing Transparency in Govt. Mid-day Meal Scheme
Inter-departmental Library Management System using Blockchain
Educational/Job Certificate Sharing and Verification using Blockchain
Adhaar-based KYC using Blockchain
College Election/Voting System Using Blockchain (Privacy+Verifiability)
Remote HealthCare System using Blockchain
Blockchain-based Platform for Judicial System to reduce delay in Justice Delivery
Visualization of Blockchain Creation: Block Creation and Mining
Multigroup Data Sharing using Blockchain and IPFS
Blockchain-based Automatic Attendance Management System (Android App)
Blockchain-based Solution to meet demand-supply and Insurance Cover in agricultural sectors