Blockchain Technology

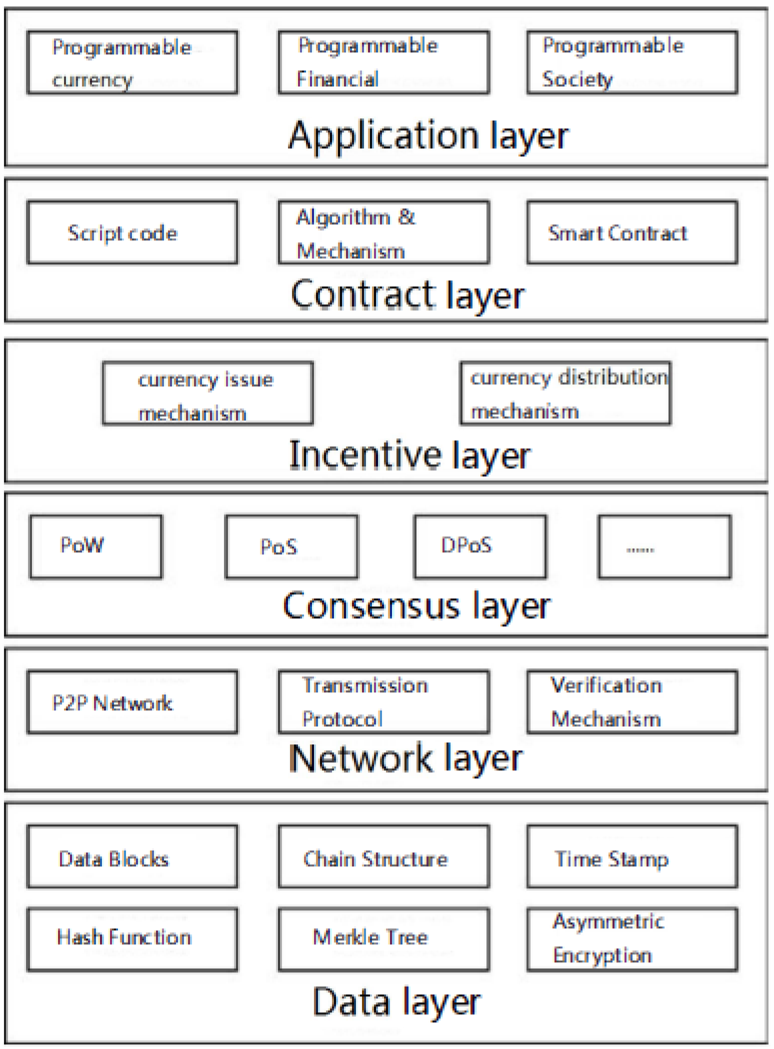
Research Directions

Blockchain Technolgy

Behind the success of Bitcoin

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

Layered Architecture



Programmable currency

Programmable Financial

Programmable Society

Application layer

Script code

Algorithm & Mechanism

Smart Contract

Contract layer

currency issue mechanism

currency distribution mechanism

Incentive layer

PoW

PoS

DPoS

......

Consensus layer

P2P Network

Transmission Protocol

Verification Mechanism

Network layer

Data Blocks

Chain Structure

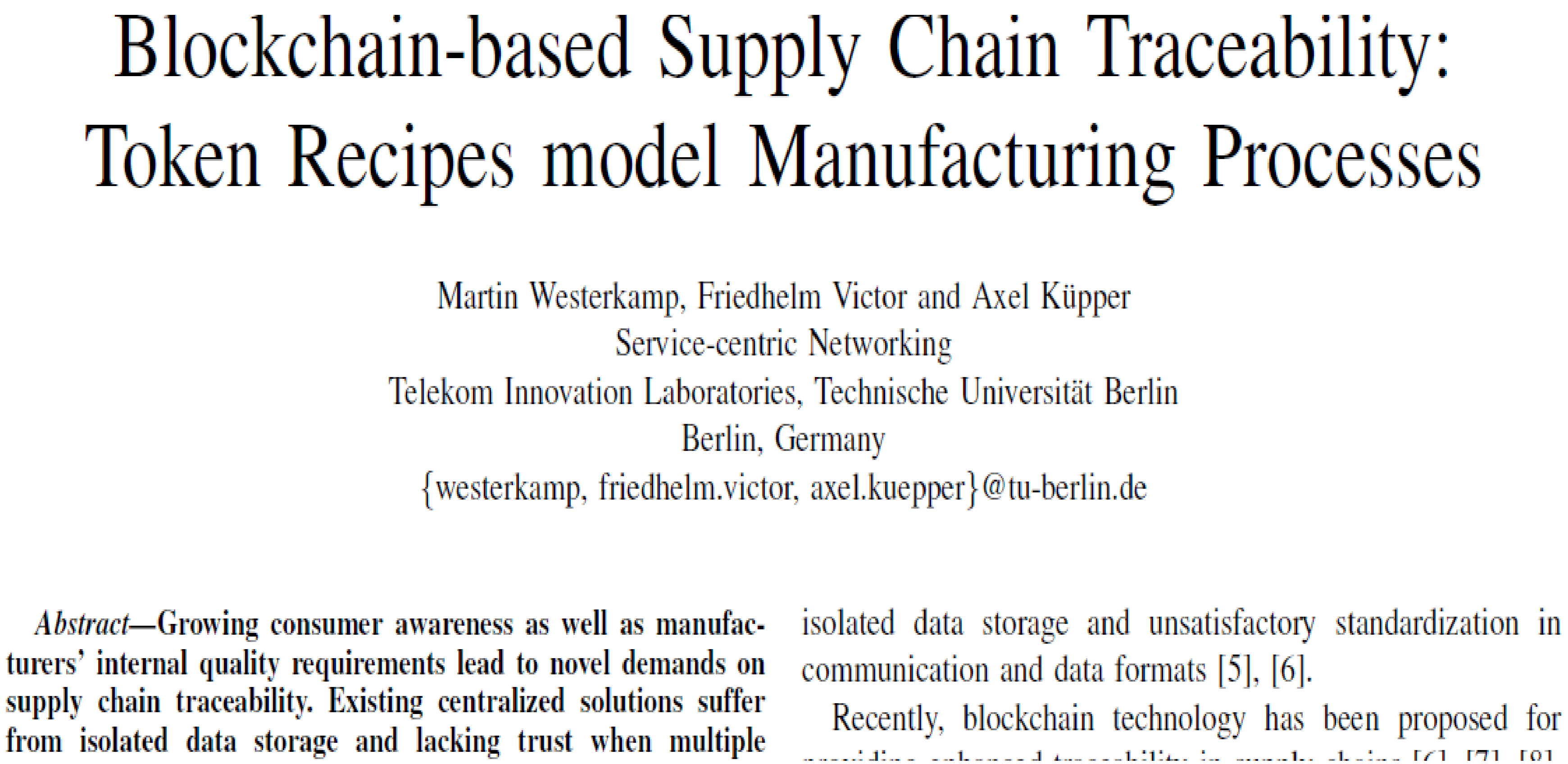
Time Stamp

Hash Function

Merkle Tree

Asymmetric Encryption

Data layer



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

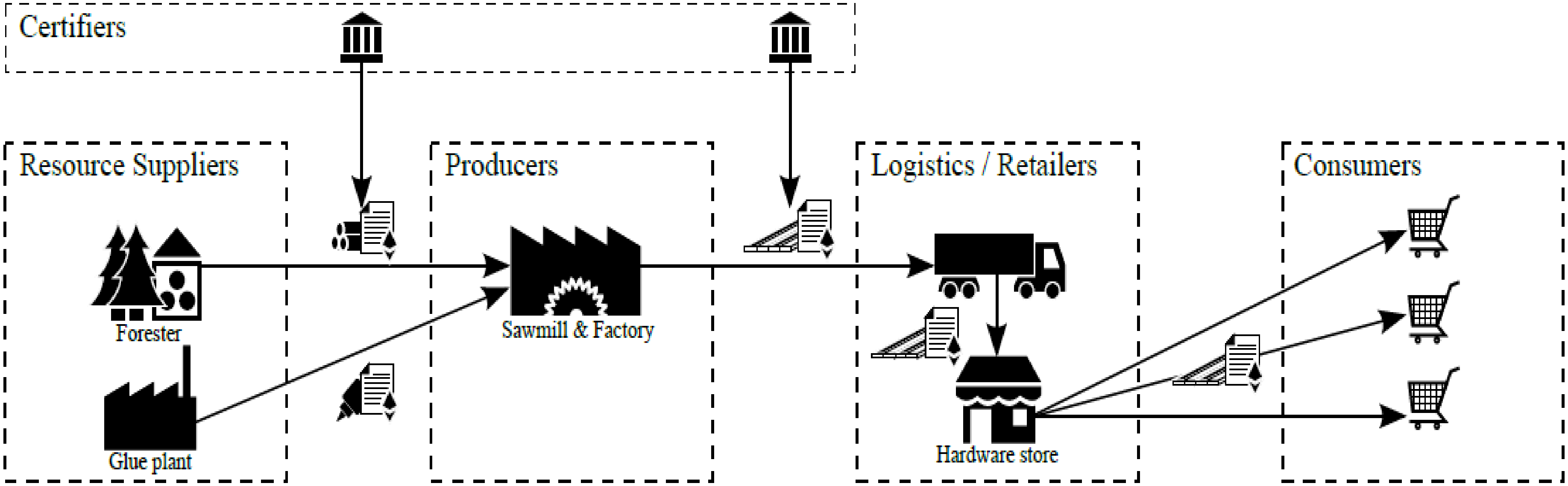
Martin Westerkamp, Friedhelm Victor and Axel Küpper
Service-centric Networking
Telekom Innovation Laboratories, Technische Universität Berlin
Berlin, Germany
{westerkamp, friedhelm.victor, axel.kuepper}@tu-berlin.de

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**

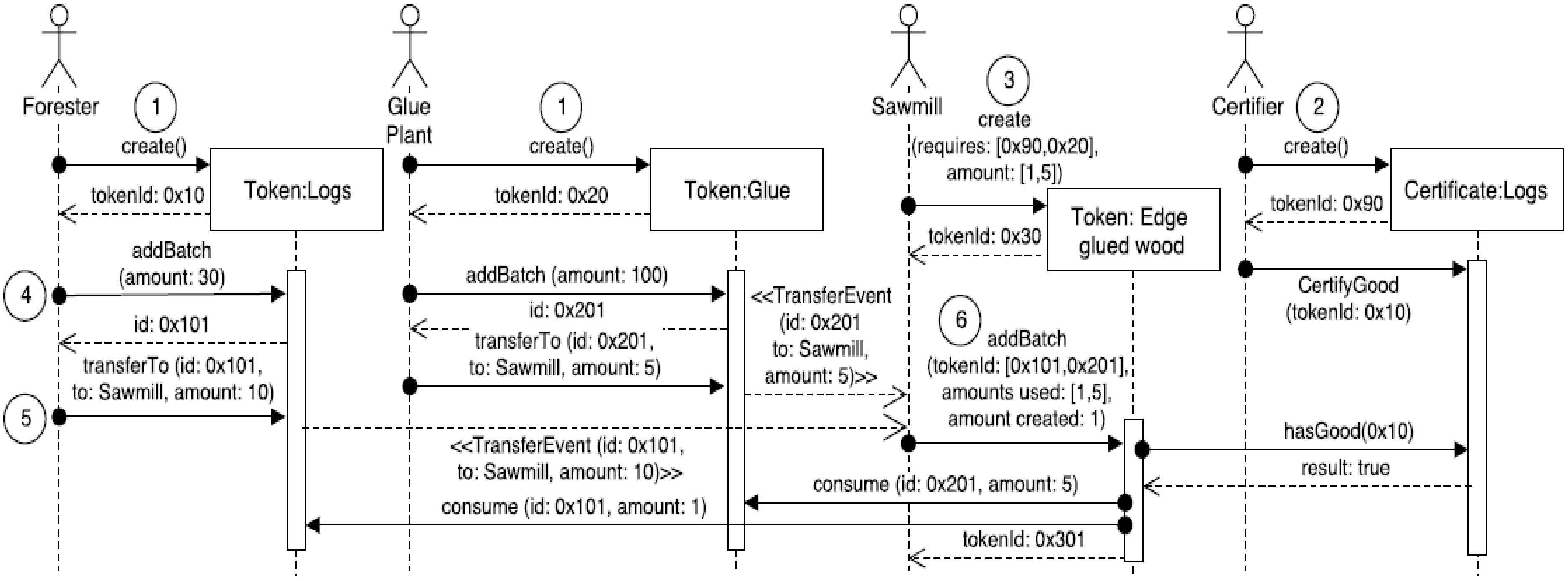
isolated data storage and unsatisfactory standardization in communication and data formats [5], [6].

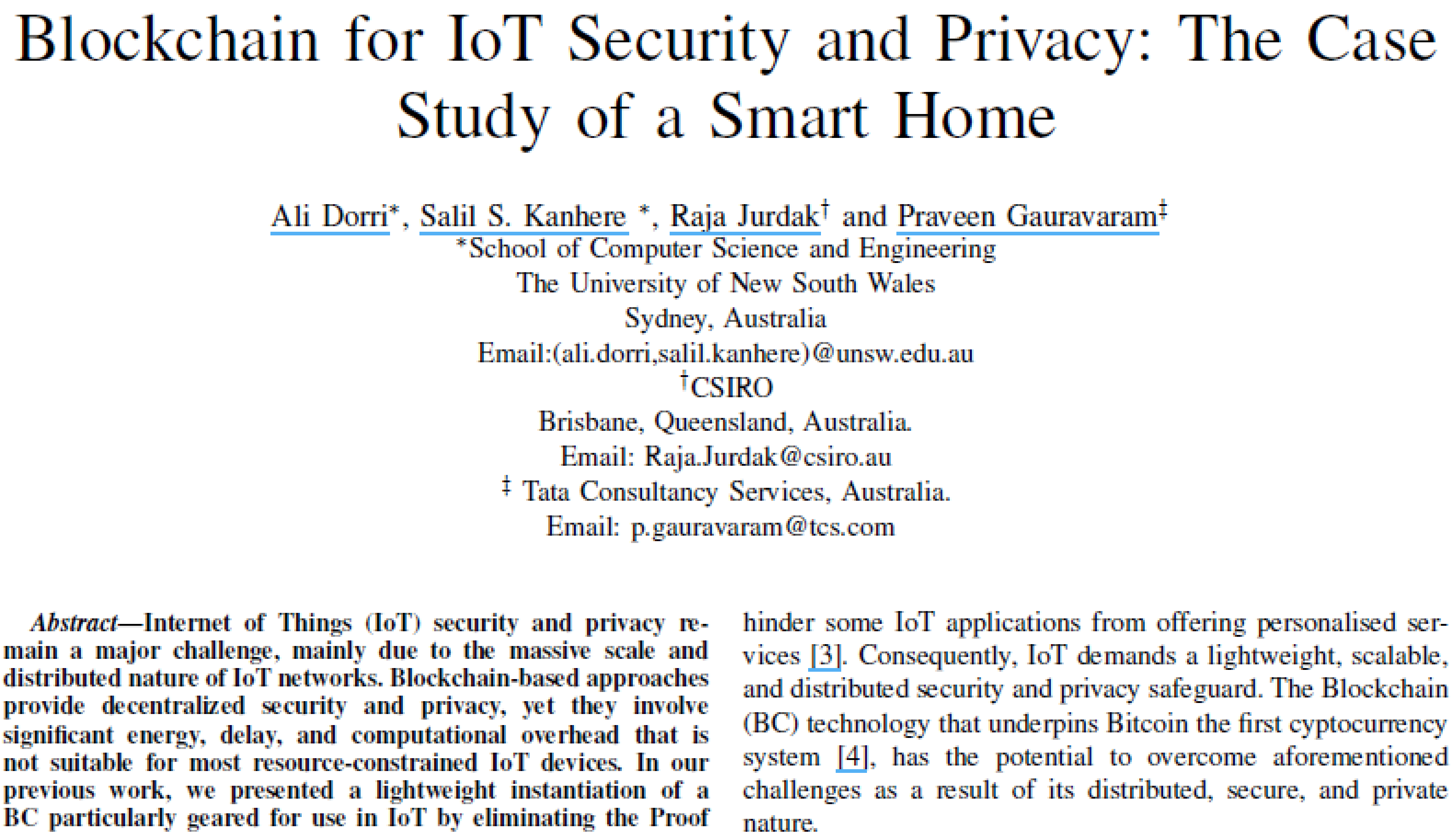
Recently, blockchain technology has been proposed for providing enhanced traceability in supply chains [6], [7], [8]

Supply Chain



Use Case of Supply Chain





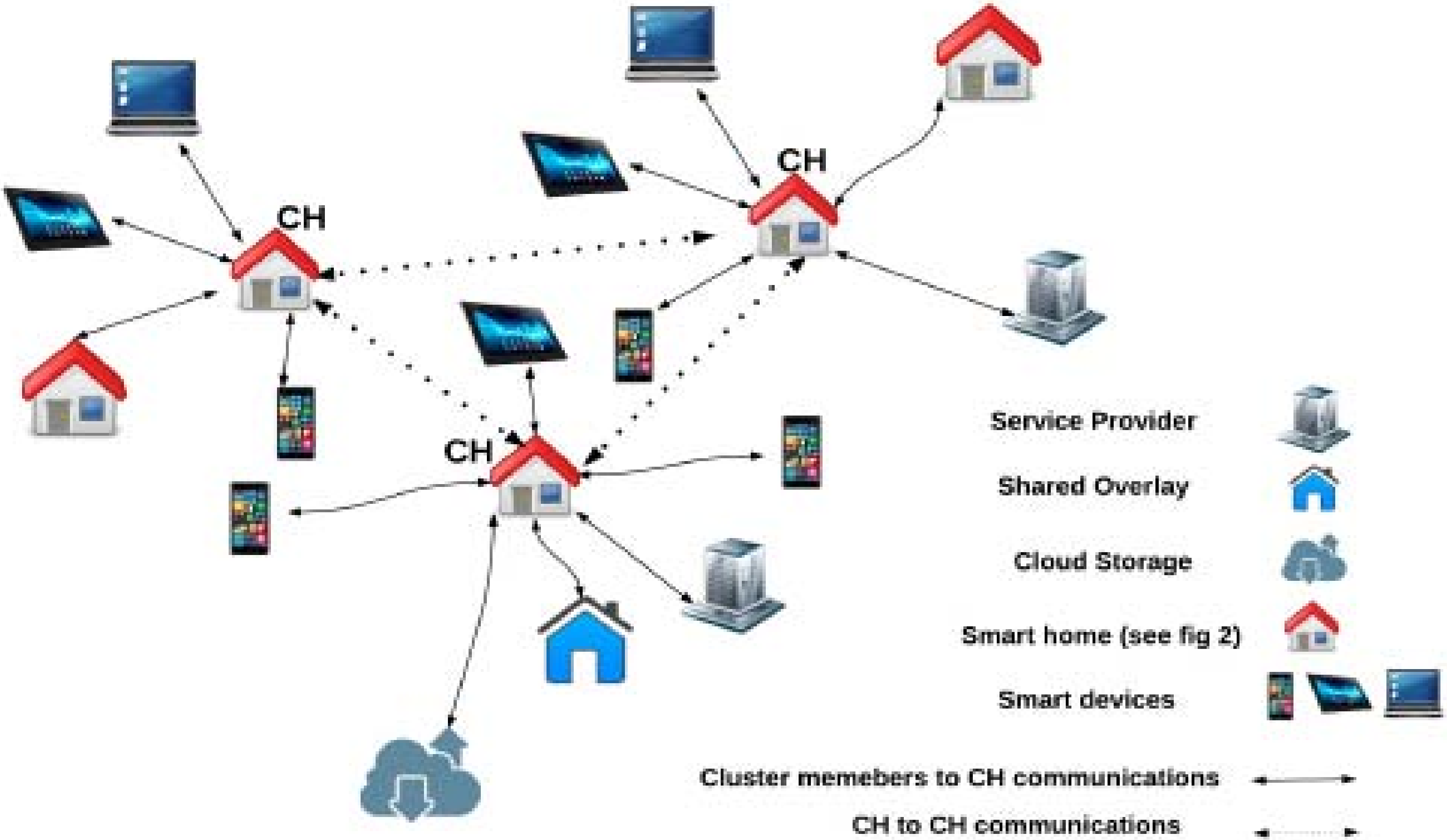
Blockchain for IoT Security and Privacy: The Case Study of a Smart Home

Ali Dorri[*], Salil S. Kanhere [*], Raja Jurdak[†] and Praveen Gauravaram[‡]
[*]School of Computer Science and Engineering
The University of New South Wales
Sydney, Australia
Email:(ali.dorri,salil.kanhere)@unsw.edu.au
[†]CSIRO
Brisbane, Queensland, Australia.
Email: Raja.Jurdak@csiro.au
[‡] Tata Consultancy Services, Australia.
Email: p.gauravaram@tcs.com

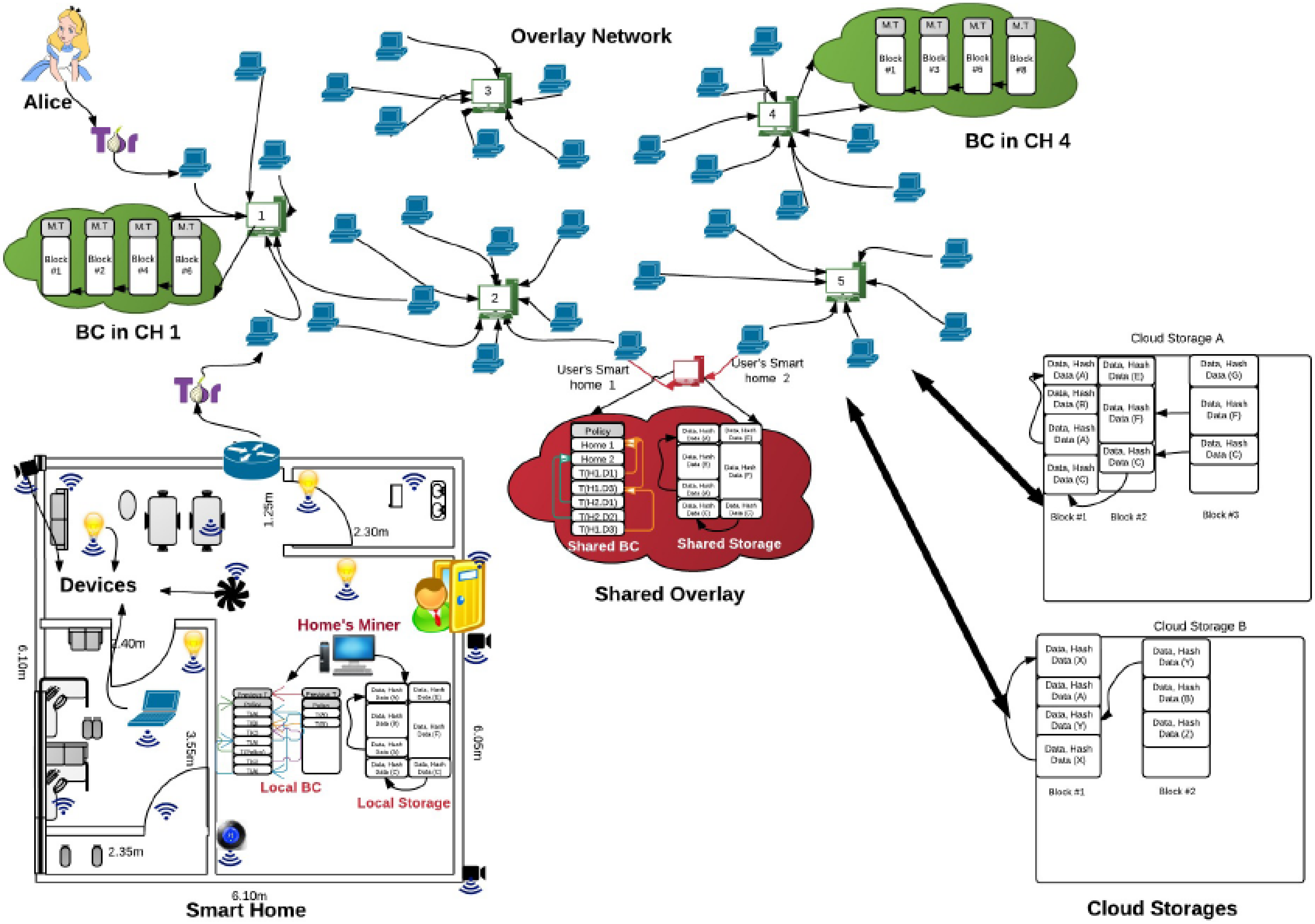
***Abstract*—Internet of Things (IoT) security and privacy remain a major challenge, mainly due to the massive scale and distributed nature of IoT networks. Blockchain-based approaches provide decentralized security and privacy, yet they involve significant energy, delay, and computational overhead that 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 cyptocurrency system [4], has the potential to overcome aforementioned challenges as a result of its distributed, secure, and private nature.

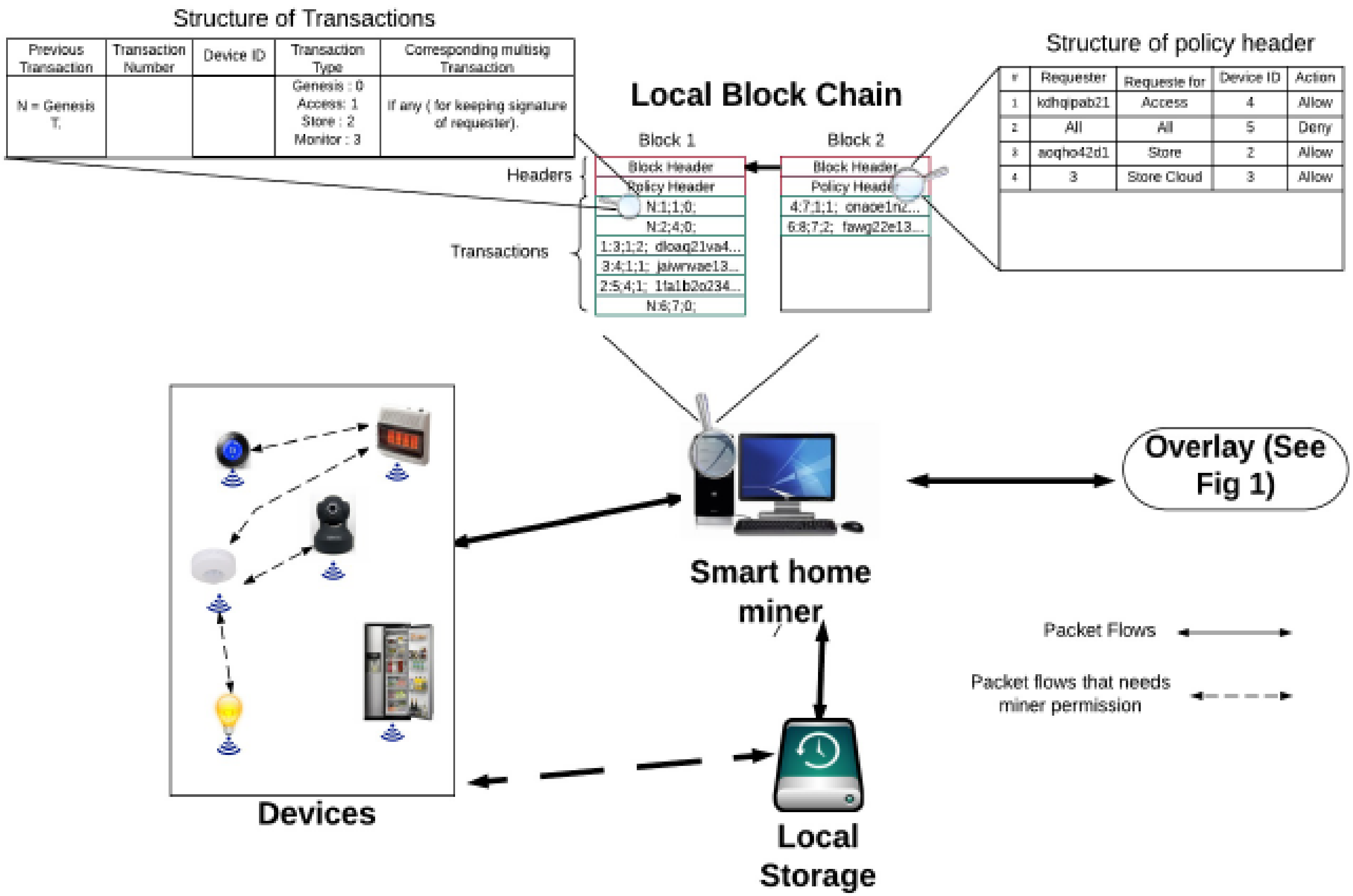
Smart Homes



CH
CH
CH
Service Provider
Shared Overlay
Cloud Storage
Smart home (see fig 2)
Smart devices
Cluster memebers to CH communications
CH to CH communications


Alice
Tor
Overlay Network
1
2
3
4
5
M.T
Block #1
Block #2
Block #4
Block #6
BC in CH 1
Block #1
Block #3
Block #5
Block #8
BC in CH 4
Tor
User's Smart home 1
User's Smart home 2
Policy
Home 1
Home 2
T(H1,D1)
T(H1,D3)
T(H2,D1)
T(H2,D2)
T(H1,D3)
Shared BC
Shared Storage
Shared Overlay
Cloud Storage A
Data, Hash Data (A)
Data, Hash Data (B)
Data, Hash Data (A)
Data, Hash Data (C)
Data, Hash Data (E)
Data, Hash Data (F)
Data, Hash Data (C)
Data, Hash Data (G)
Data, Hash Data (F)
Data, Hash Data (C)
Block #1
Block #2
Block #3
Cloud Storage B
Data, Hash Data (X)
Data, Hash Data (A)
Data, Hash Data (Y)
Data, Hash Data (X)
Data, Hash Data (Y)
Data, Hash Data (B)
Data, Hash Data (Z)
Block #1
Block #2
Cloud Storages
1.25m
2.30m
Devices
Home's Miner
2.40m
6.10m
3.55m
6.05m
Local BC
Local Storage
2.35m
6.10m
Smart Home

Smart Homes



Structure of Transactions

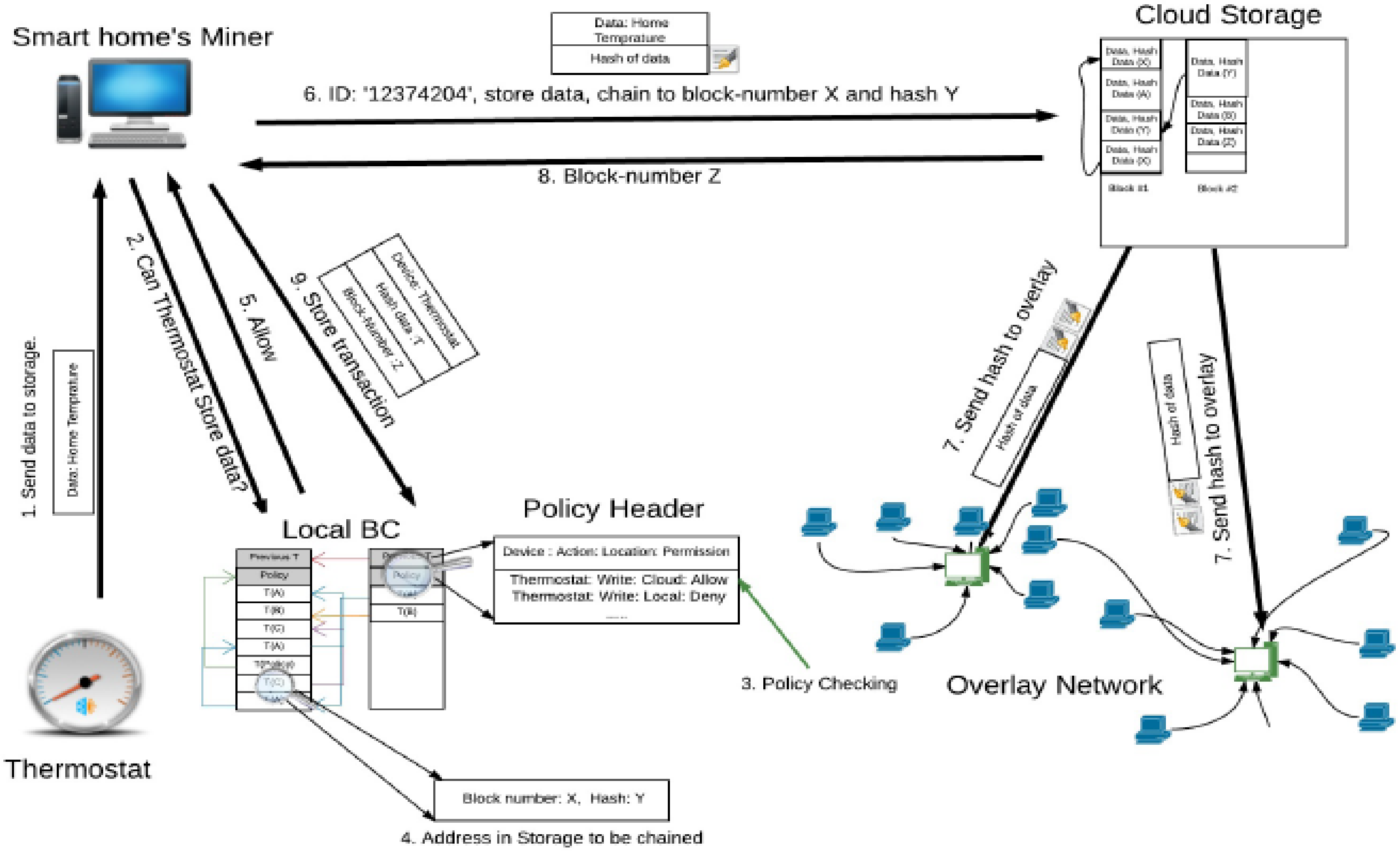
Previous Transaction	Transaction Number	Device ID	Transaction Type	Corresponding multisig Transaction
N = Genesis T,			Genesis : 0 Access: 1 Store : 2 Monitor : 3	If any (for keeping signature of requester).

Structure of policy header

#	Requester	Requeste for	Device ID	Action
1	kdhqipab21	Access	4	Allow
2	All	All	5	Deny
3	aoqho42d1	Store	2	Allow
4	3	Store Cloud	3	Allow

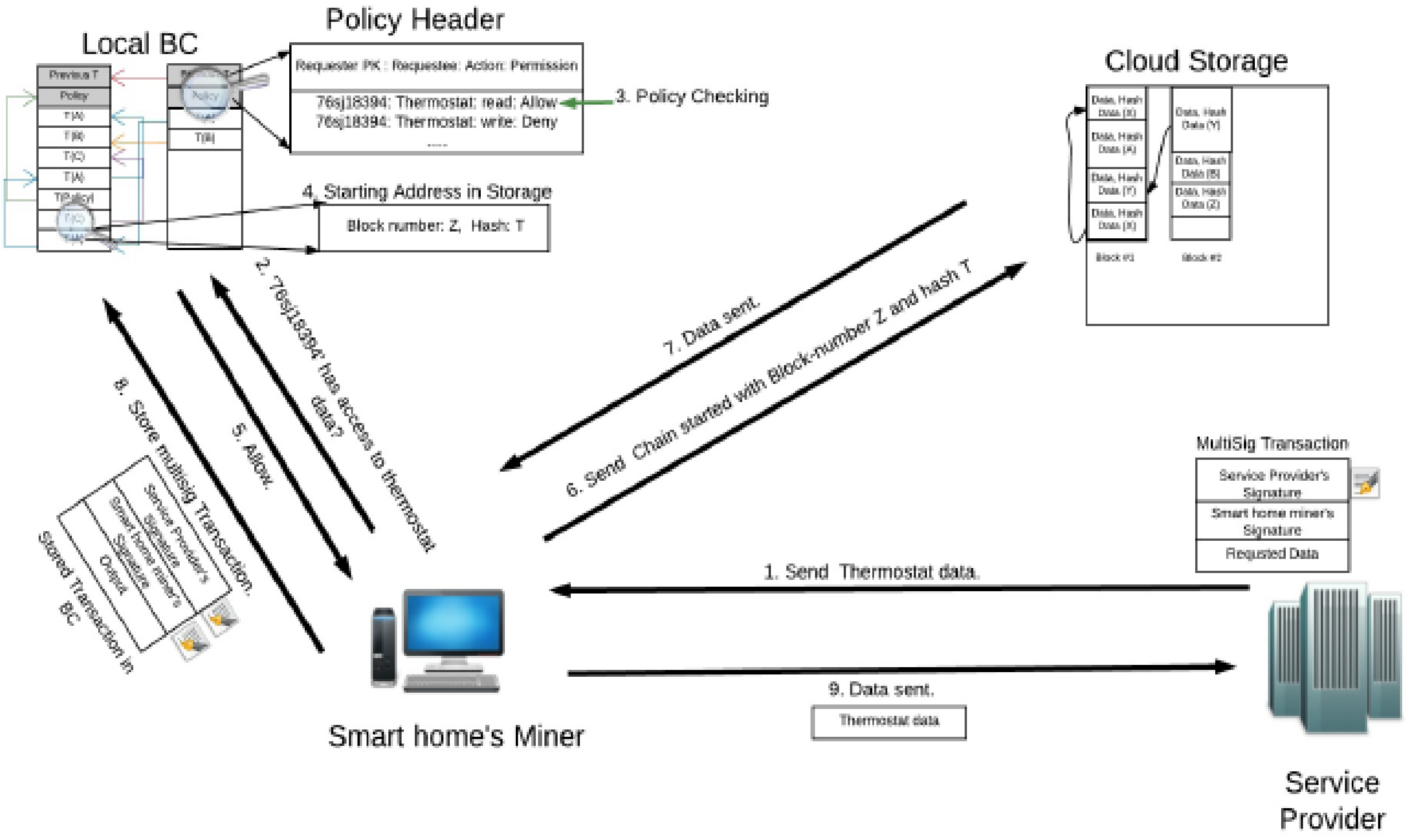
Smart Homes

Store Transaction



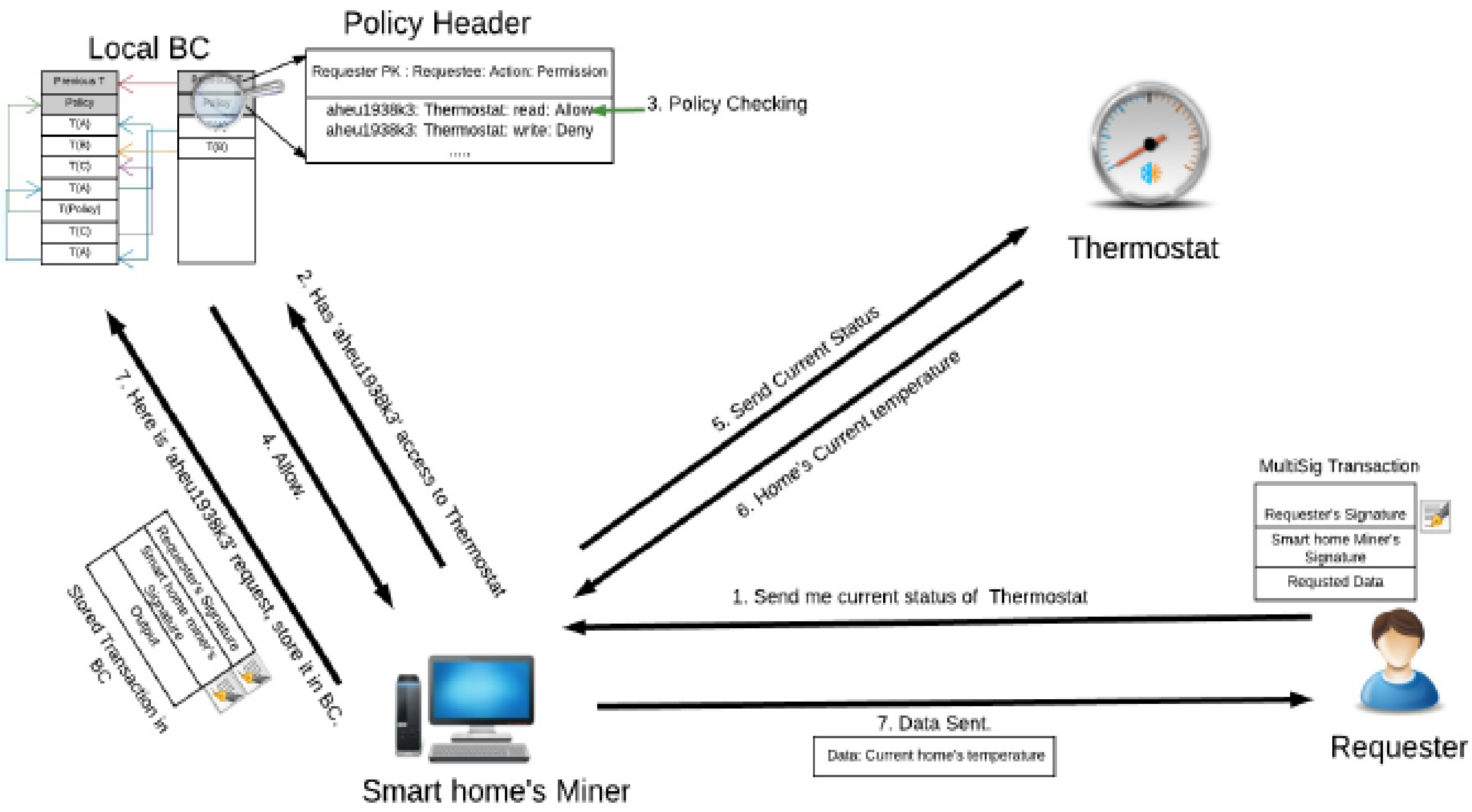
Smart Homes

Access Transaction



Smart Homes

Monitor Transaction


Local BC
Previous T
Policy
T(A)
T(B)
T(C)
T(A)
T(Policy)
T(C)
T(A)
Policy
T(B)
Policy Header
Requester PK : Requestee: Action: Permission
aheu1938k3: Thermostat: read: Allow
aheu1938k3: Thermostat: write: Deny
.....
3. Policy Checking
Thermostat
2. Has 'aheu1938k3' access to Thermostat
4. Allow.
7. Here is 'aheu1938k3' request, store it in BC.
Requester's Signature
Smart home miner's Signature
Output
Stored Transaction in BC
5. Send Current Status
6. Home's Current temperature
MultiSig Transaction
Requester's Signature
Smart home Miner's Signature
Requsted Data
1. Send me current status of Thermostat
7. Data Sent.
Data: Current home's temperature
Smart home's Miner
Requester

2016 2nd IEEE International Conference on Computer and Communications

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

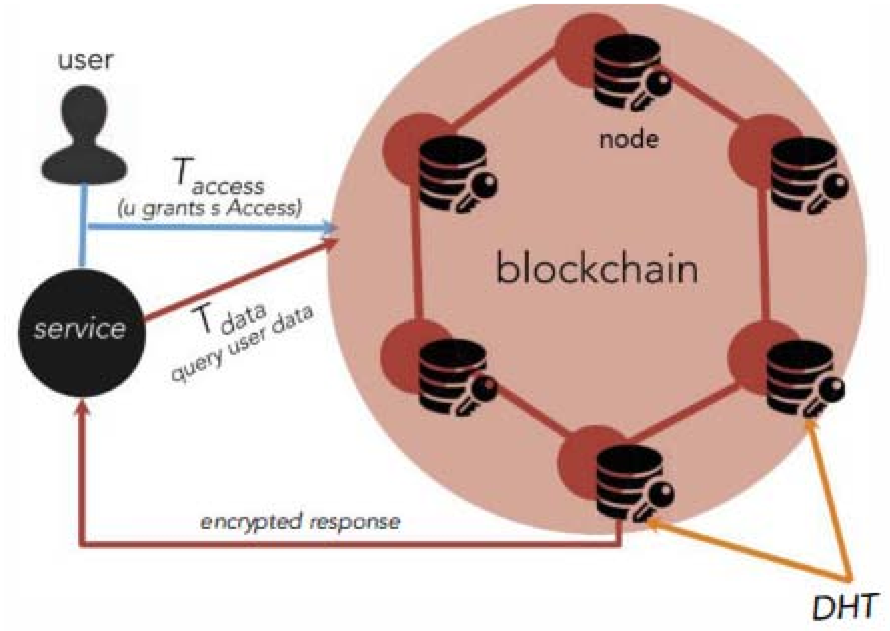
***Abstract*—MIT Media Lab employed blockchain to describe a decentralized personal data management system (i.e. Decentralizing Privacy) that ensures users own and control their data without authentication from a third party. In this paper, we employ a better encryption algorithm from NTT Service Evolution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

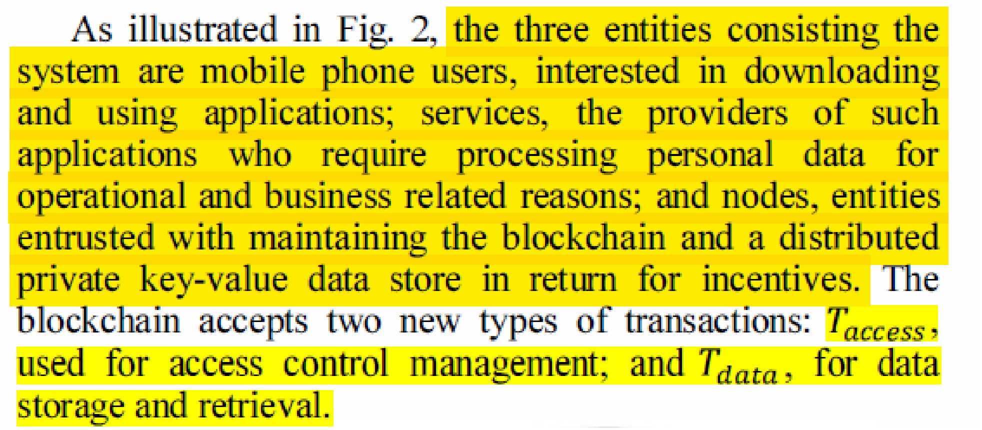
Today, data is a valuable asset in our economy [7]. Facebook, the largest online social-network, collected 300 petabytes of personal data since its inception – a hundred times the amount the Library of Congress has collected in over 200 years [8].

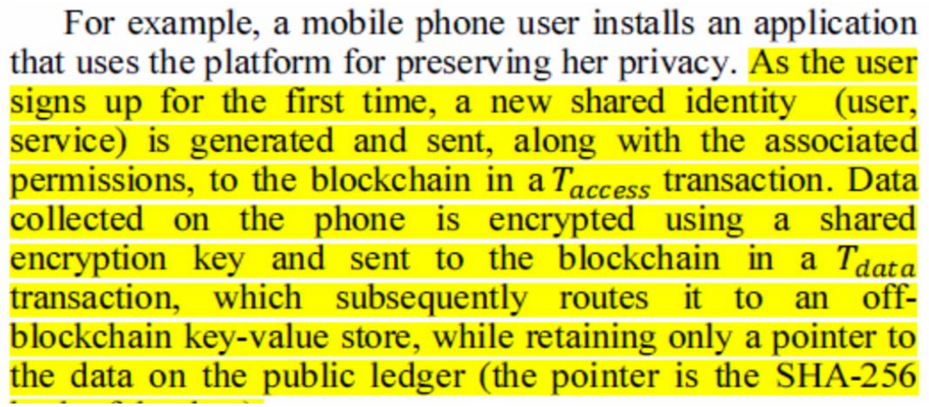
In recent years, a new class of accountable systems

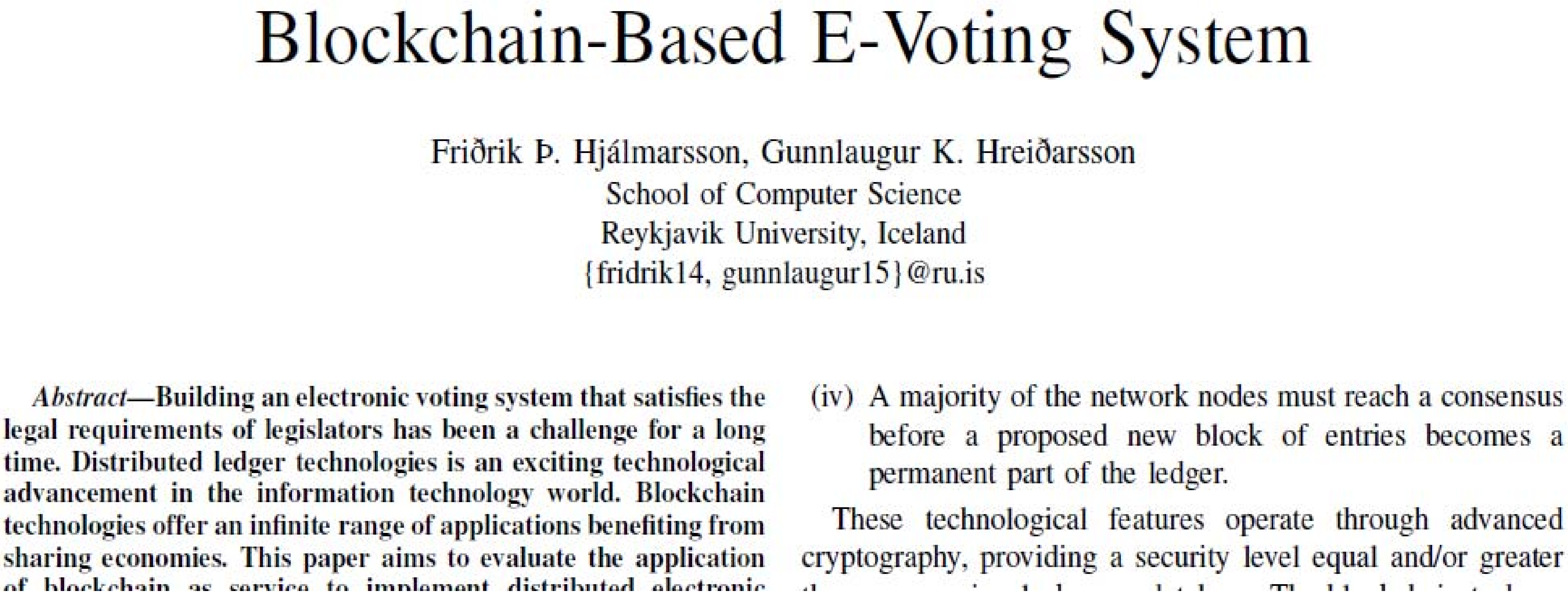
Data Privacy Management (at MIT)

- 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.


For example, a mobile phone user installs an application that uses the platform for preserving her privacy. As the user signs up for the first time, a new shared identity (user, service) is generated and sent, along with the associated permissions, to the blockchain in a T_{access} transaction. Data collected on the phone is encrypted using a shared encryption key and sent to the blockchain in a T_{data} transaction, which subsequently routes it to an off-blockchain key-value store, while retaining only a pointer to the data on the public ledger (the pointer is the SHA-256



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

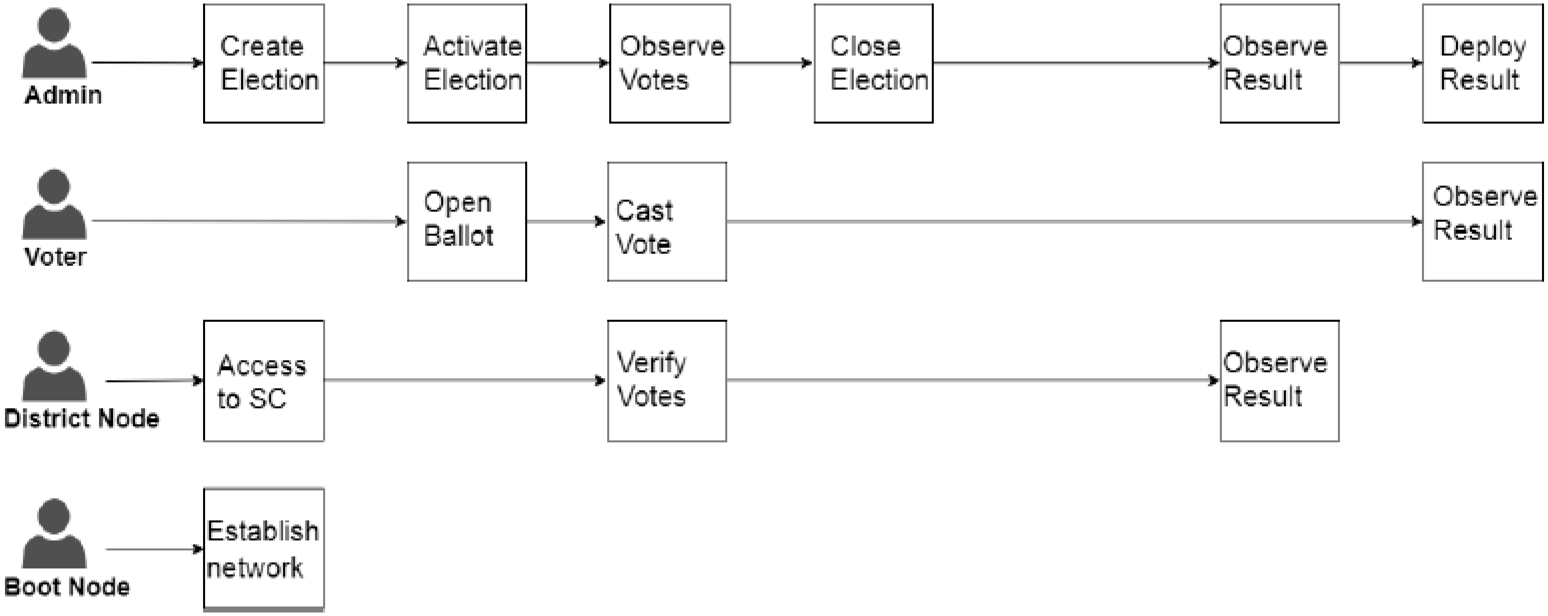
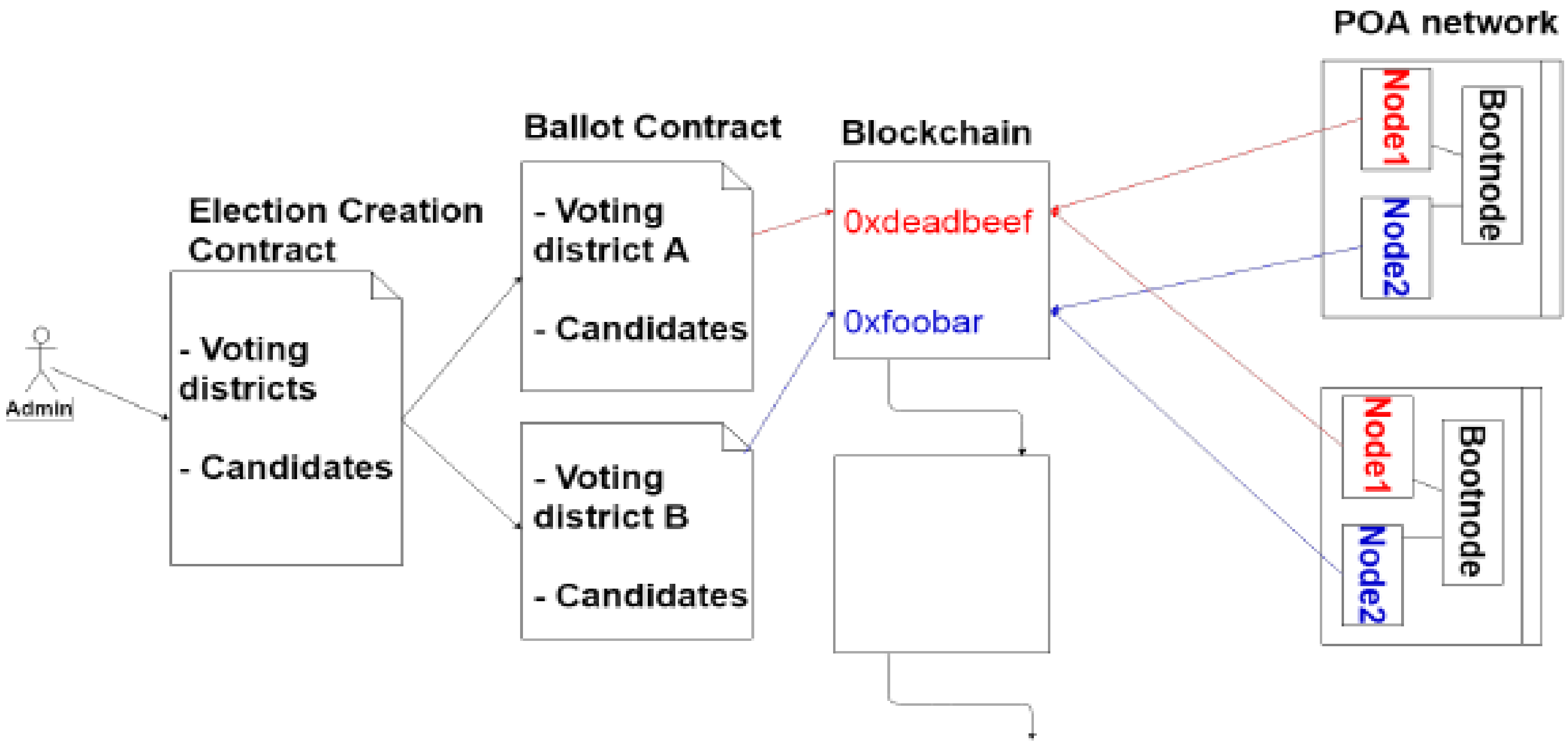


Fig. 1: Election roles and process

Election as Smart Contract



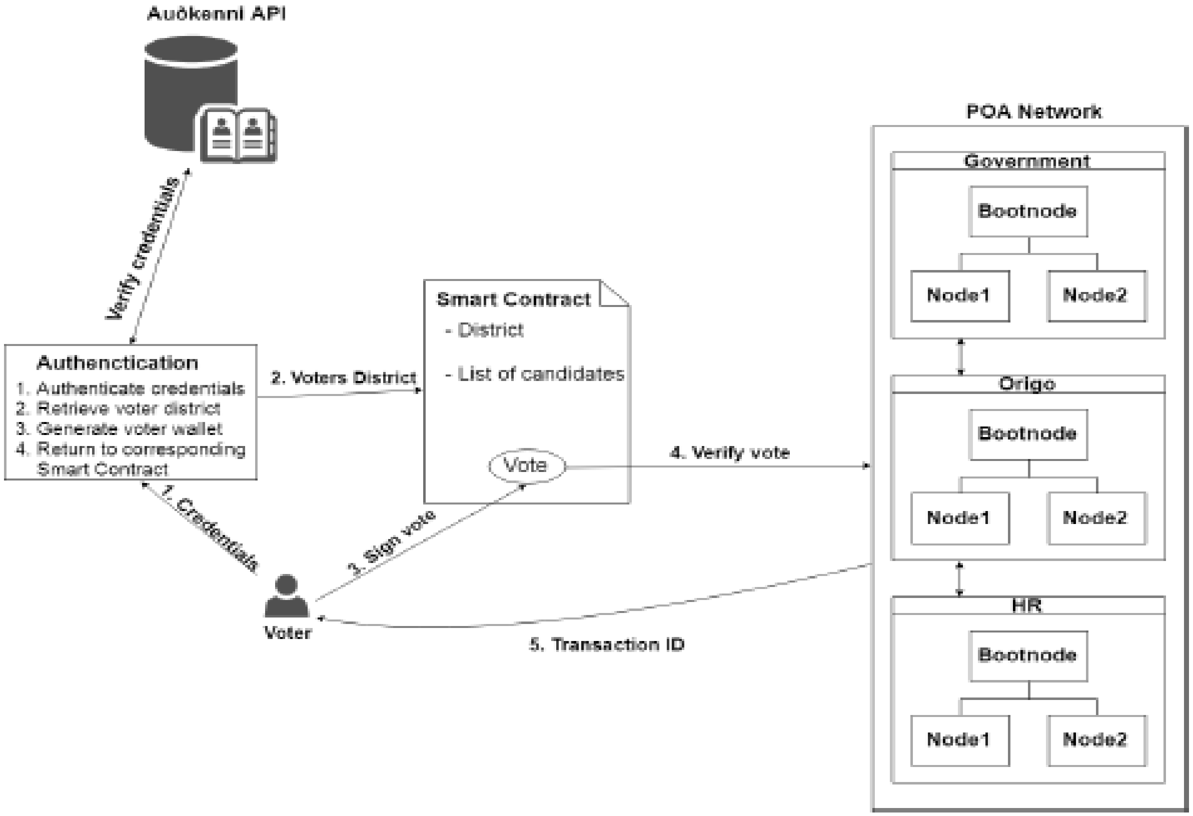


Fig. 3: Voter authenticates himself and casts vote

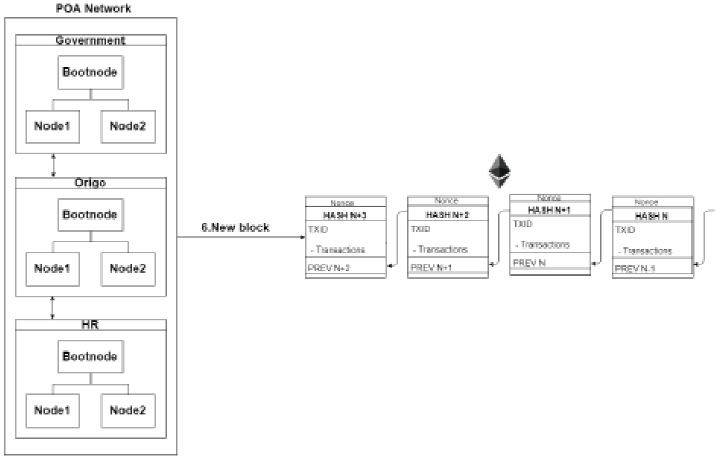
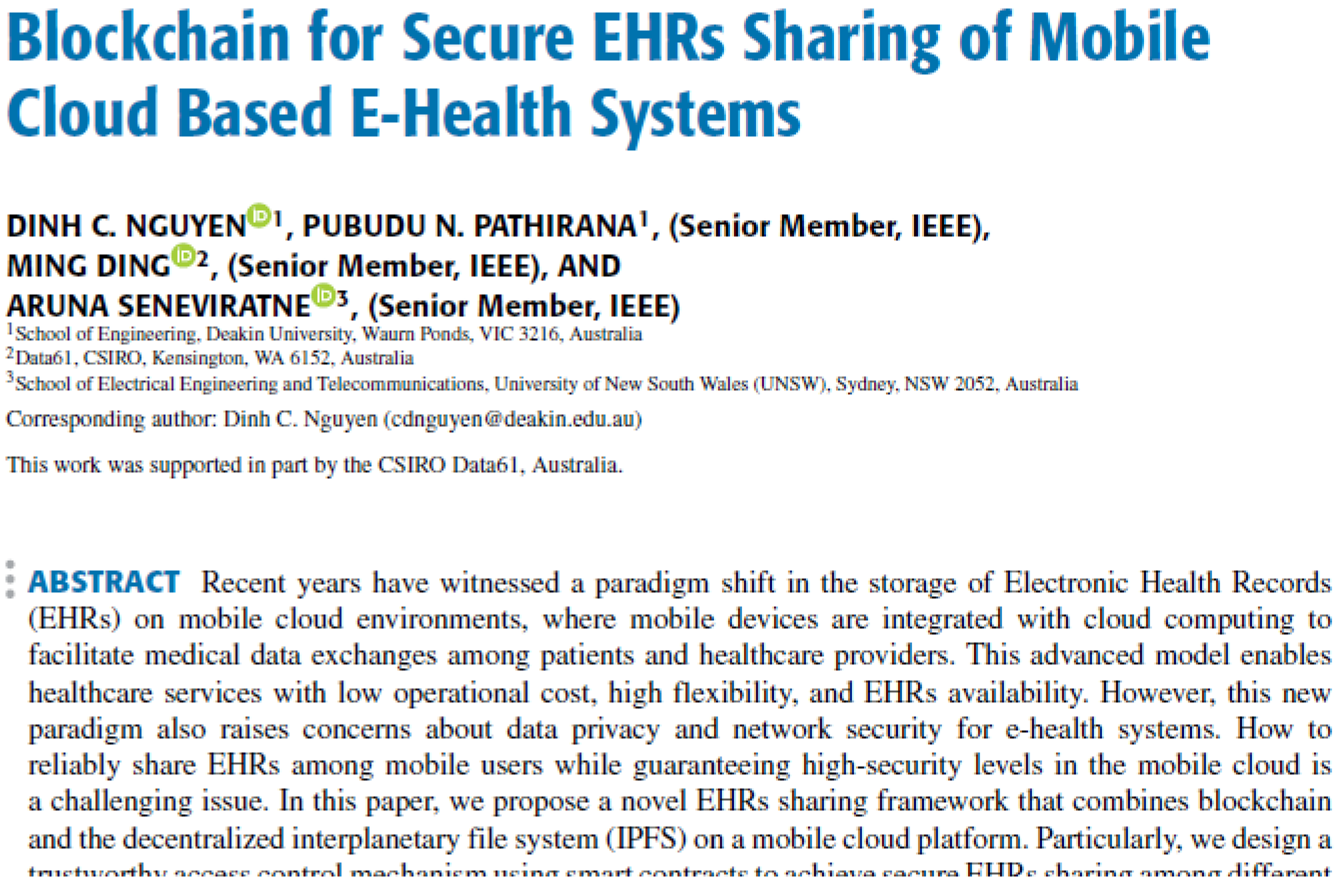


Fig. 4: Block added to the blockchain



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

DINH C. NGUYEN[1], PUBUDU N. PATHIRANA[1], (Senior Member, IEEE), MING DING[2], (Senior Member, IEEE), AND ARUNA SENEVIRATNE[3], (Senior Member, IEEE)

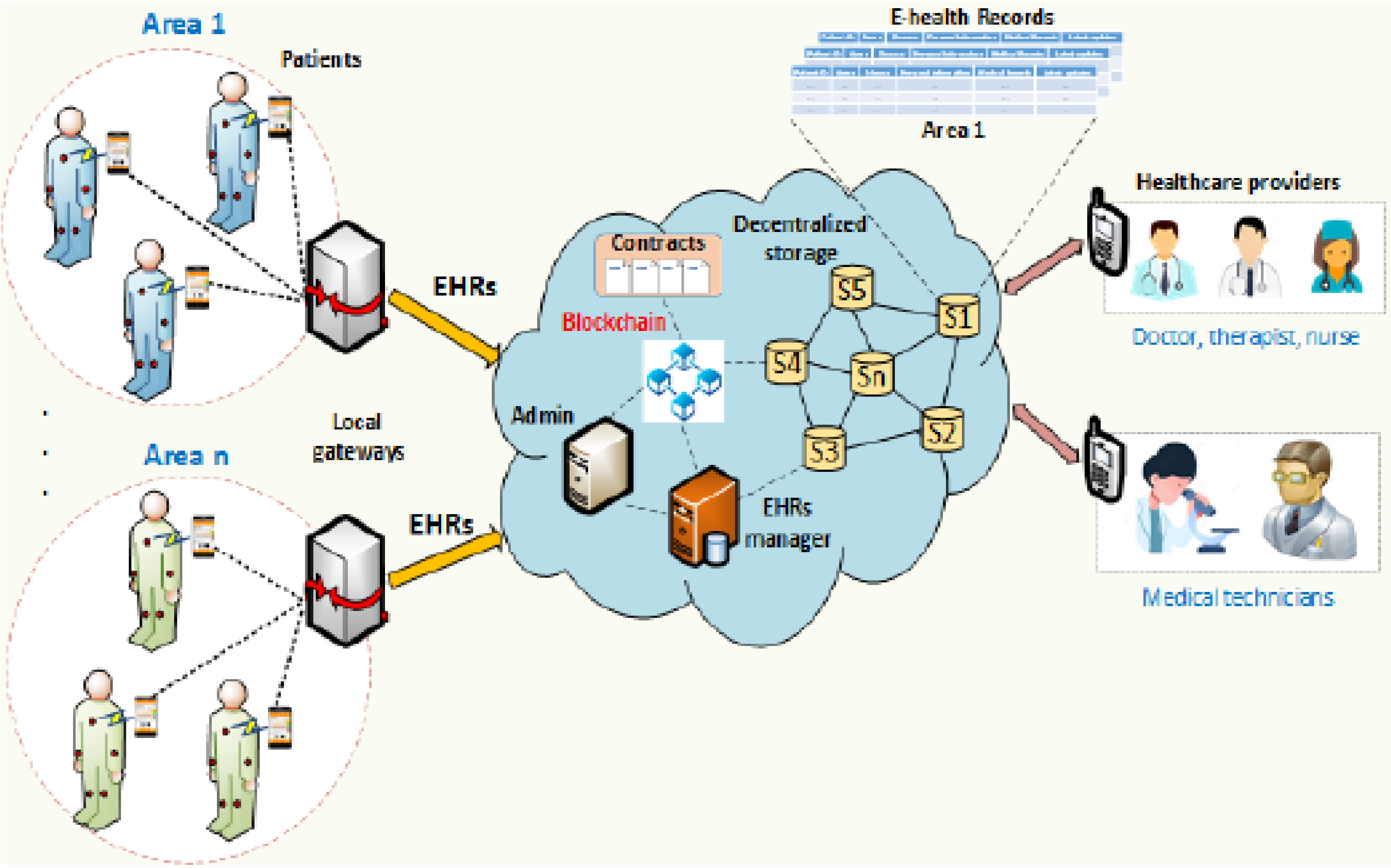
[1]School of Engineering, Deakin University, Waurn Ponds, VIC 3216, Australia
[2]Data61, CSIRO, Kensington, WA 6152, Australia
[3]School of Electrical Engineering and Telecommunications, University of New South Wales (UNSW), Sydney, NSW 2052, Australia

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

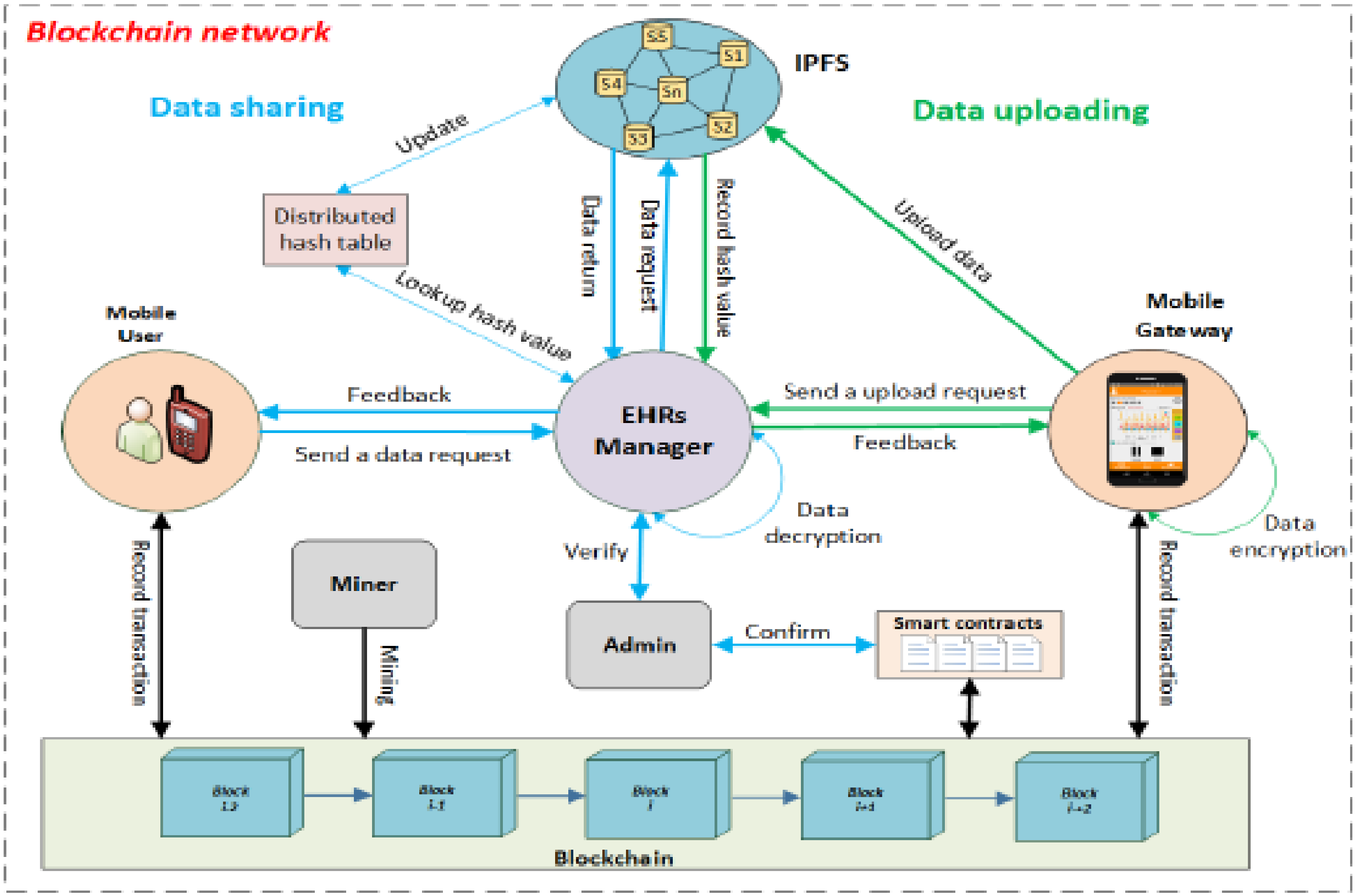
This work was supported in part by the CSIRO Data61, Australia.

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


Area 1
Patients
Local
gateways
Area n
EHRs
EHRs
E-health Records
Area 1
Contracts
Decentralized
storage
Blockchain
Admin
EHRs
manager
S1
S2
S3
S4
S5
Sn
Healthcare providers
Doctor, therapist, nurse
Medical technicians

HealthCare


Blockchain network
IPFS
S5
S1
S4
Sn
S2
S3
Data sharing
Data uploading
Update
Distributed hash table
Lookup hash value
Data return
Data request
Record hash value
Upload data
Mobile User
Mobile Gate way
Feedback
Send a data request
EHRs Manager
Send a upload request
Feedback
Data decryption
Data encryption
Verify
Miner
Mining
Admin
Confirm
Smart contracts
Record transaction
Record transaction
Block i-2
Block i-1
Block i
Block i+1
Block i+2
Blockchain

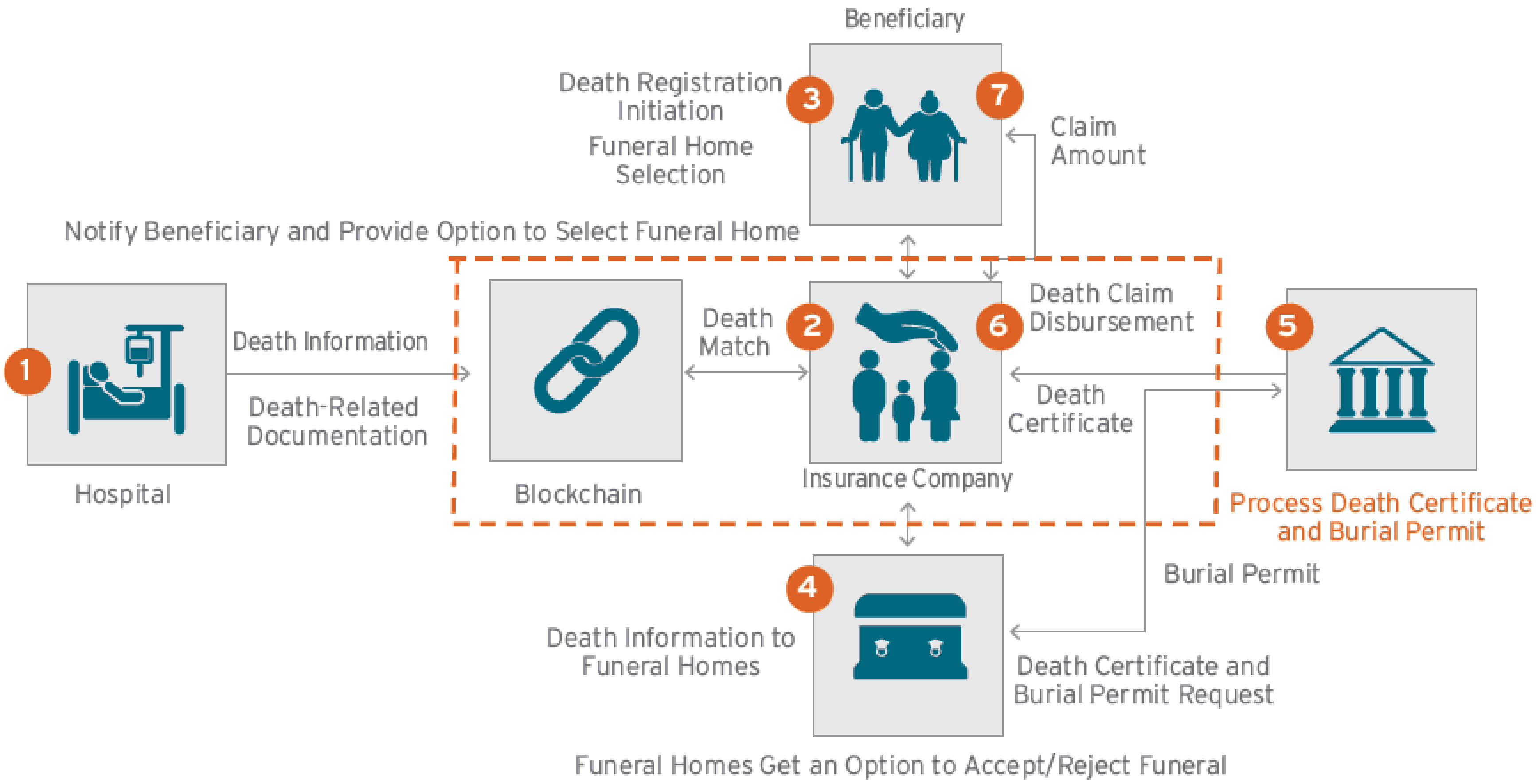
Cognizant

DIGITAL SYSTEMS & TECHNOLOGY

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!


Beneficiary
3
Death Registration Initiation
Funeral Home Selection
7
Claim Amount
Notify Beneficiary and Provide Option to Select Funeral Home
1
Hospital
Death Information
Death-Related Documentation
Blockchain
Death Match
2
6
Insurance Company
Death Claim Disbursement
Death Certificate
5
Process Death Certificate and Burial Permit
Burial Permit
4
Death Information to Funeral Homes
Death Certificate and Burial Permit Request
Funeral Homes Get an Option to Accept/Reject Funeral

https://www.thewindowsclub.com/decentralized-social-networks/amp

Decentralised Social Network

1] Diaspora (diasporafoundation.org)

2] SocialX (socialx.network)

3] Minds (wefunder.com/minds)

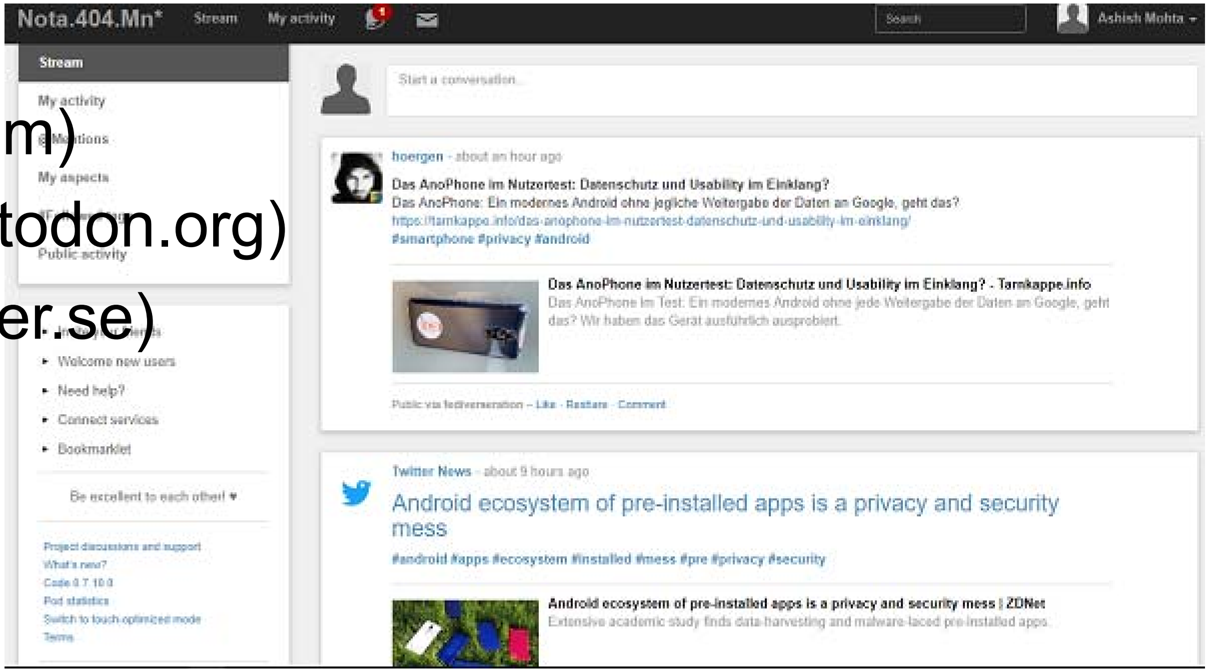
4] Memo (memo.cash)

5] Sola (sola.ai)

6] Steemit (steemit.com)

7] Mastodon (joinmastodon.org)

8] Manyverse (manyver.se)



hoergen - about an hour ago

Das AnoPhone im Nutzertest: Datenschutz und Usability im Einklang?
Das AnoPhone: Ein modernes Android ohne jegliche Weitergabe der Daten an Google, geht das?
https://tarnkappe.info/das-anophone-im-nutzertest-datenschutz-und-usability-im-einklang/
#smartphone #privacy #android

Das AnoPhone im Nutzertest: Datenschutz und Usability im Einklang? - Tarnkappe.info
Das AnoPhone im Test: Ein modernes Android ohne jede Weitergabe der Daten an Google, geht das? Wir haben das Gerät ausführlich ausprobiert.

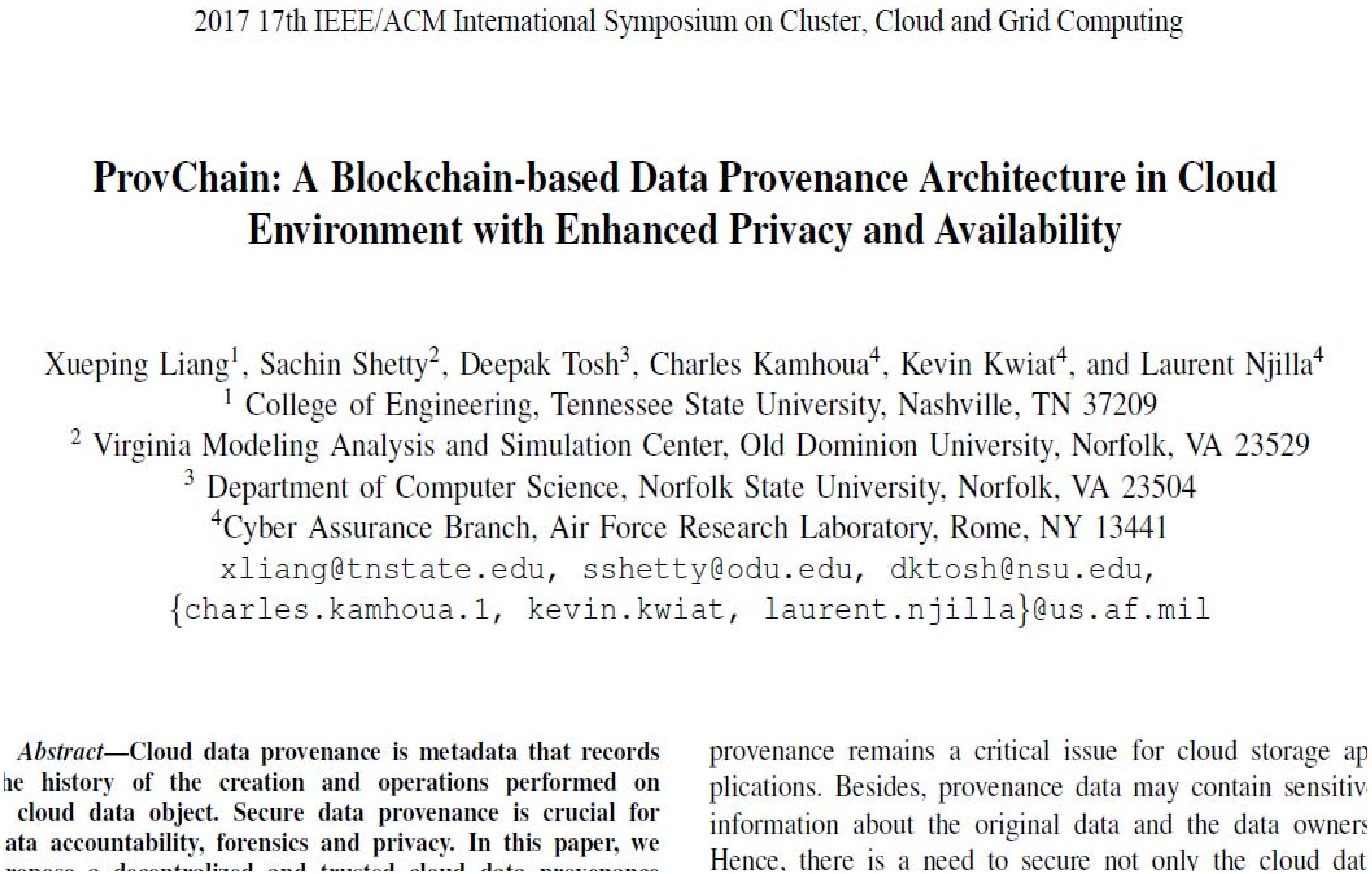
Public via fediverseration – Like · Reshare · Comment

Twitter News - about 9 hours ago

Android ecosystem of pre-installed apps is a privacy and security mess

#android #apps #ecosystem #installed #mess #pre #privacy #security

Android ecosystem of pre-installed apps is a privacy and security mess | ZDNet
Extensive academic study finds data-harvesting and malware-laced pre-installed apps.



2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing

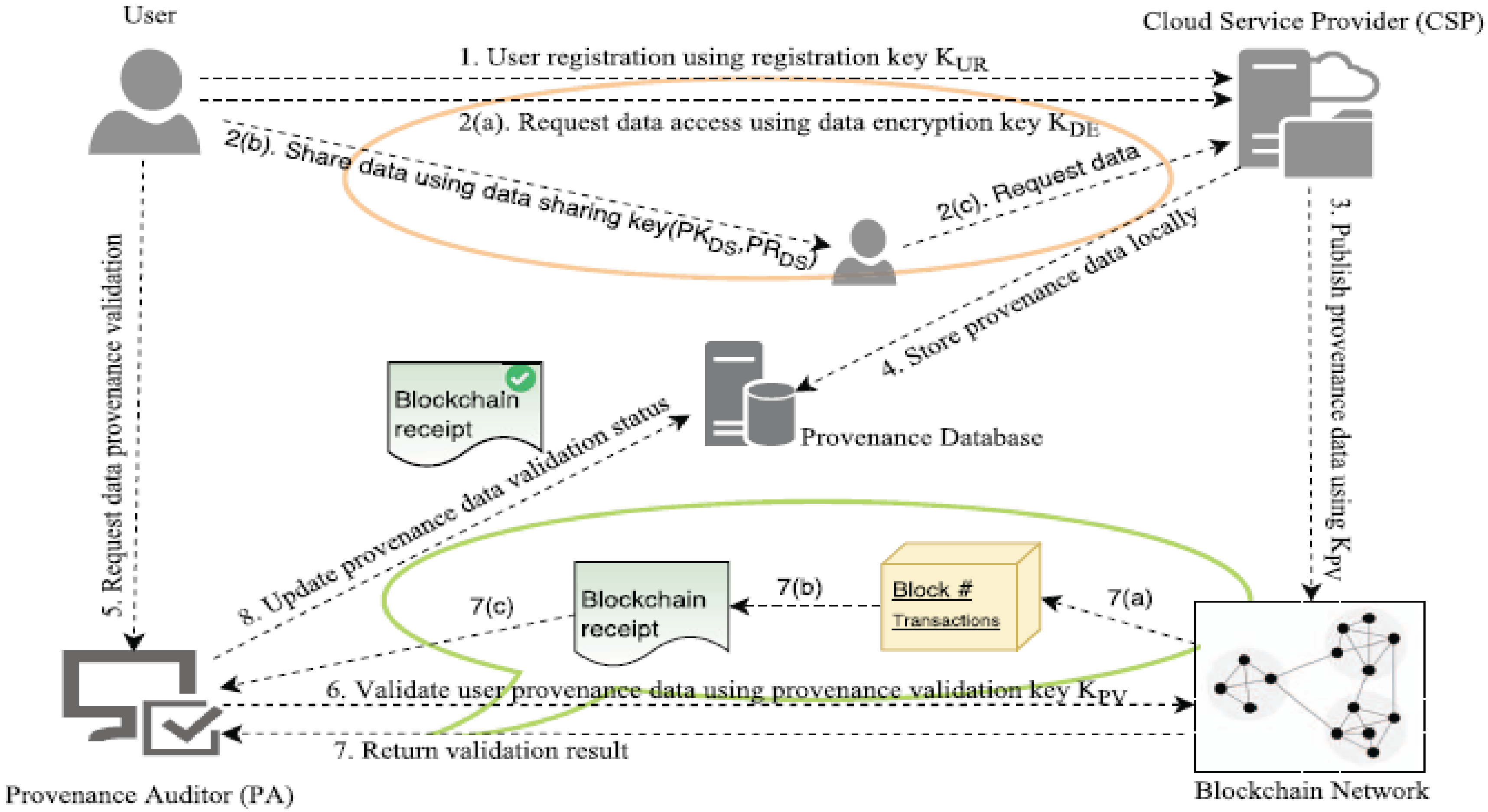
ProvChain: A Blockchain-based Data Provenance Architecture in Cloud Environment with Enhanced Privacy and Availability

Xueping Liang[1], Sachin Shetty[2], Deepak Tosh[3], Charles Kamhoua[4], Kevin Kwiat[4], and Laurent Njilla[4]
[1] College of Engineering, Tennessee State University, Nashville, TN 37209
[2] Virginia Modeling Analysis and Simulation Center, Old Dominion University, Norfolk, VA 23529
[3] Department of Computer Science, Norfolk State University, Norfolk, VA 23504
[4]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 he history of the creation and operations performed on cloud data object. Secure data provenance is crucial for ata accountability, forensics and privacy. In this paper, we**

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

Blockchain-based Data Provenance in Cloud



User

Cloud Service Provider (CSP)

1. User registration using registration key K_{UR}

2(a). Request data access using data encryption key K_{DE}

2(b). Share data using data sharing key(PK_{DS},PR_{DS})

2(c). Request data

3. Publish provenance data using K_{PV}

4. Store provenance data locally

Provenance Database

Blockchain receipt

5. Request data provenance validation

6. Validate user provenance data using provenance validation key K_{PV}

7. Return validation result

7(a)

7(b)

7(c)

Block #

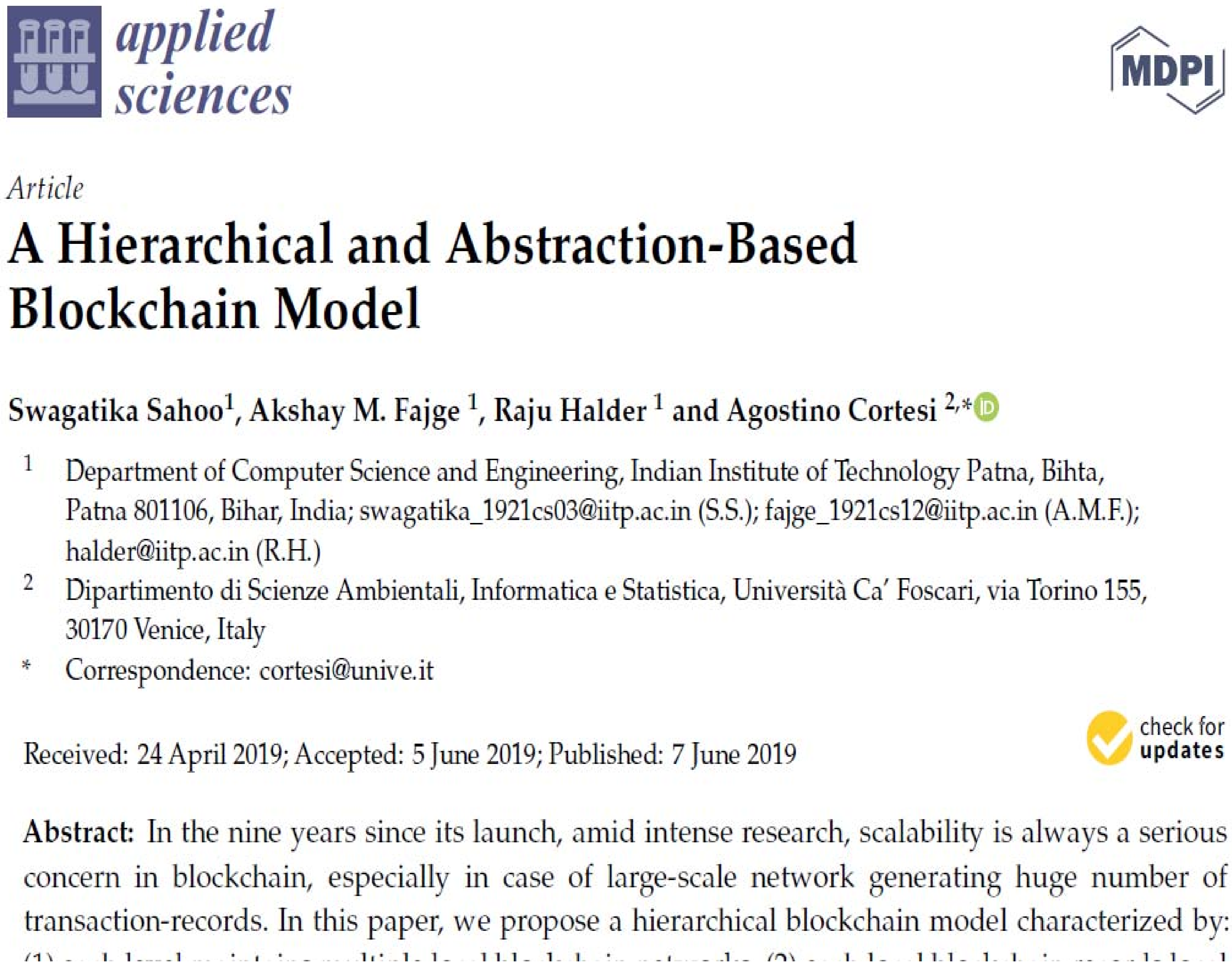
Transactions

Blockchain receipt

8. Update provenance data validation status

Provenance Auditor (PA)

Blockchain Network



applied sciences

MDPI

Article

A Hierarchical and Abstraction-Based Blockchain Model

Swagatika Sahoo[1], Akshay M. Fajge [1], Raju Halder [1] and Agostino Cortesi [2,*]

[1] 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.)

[2] 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:

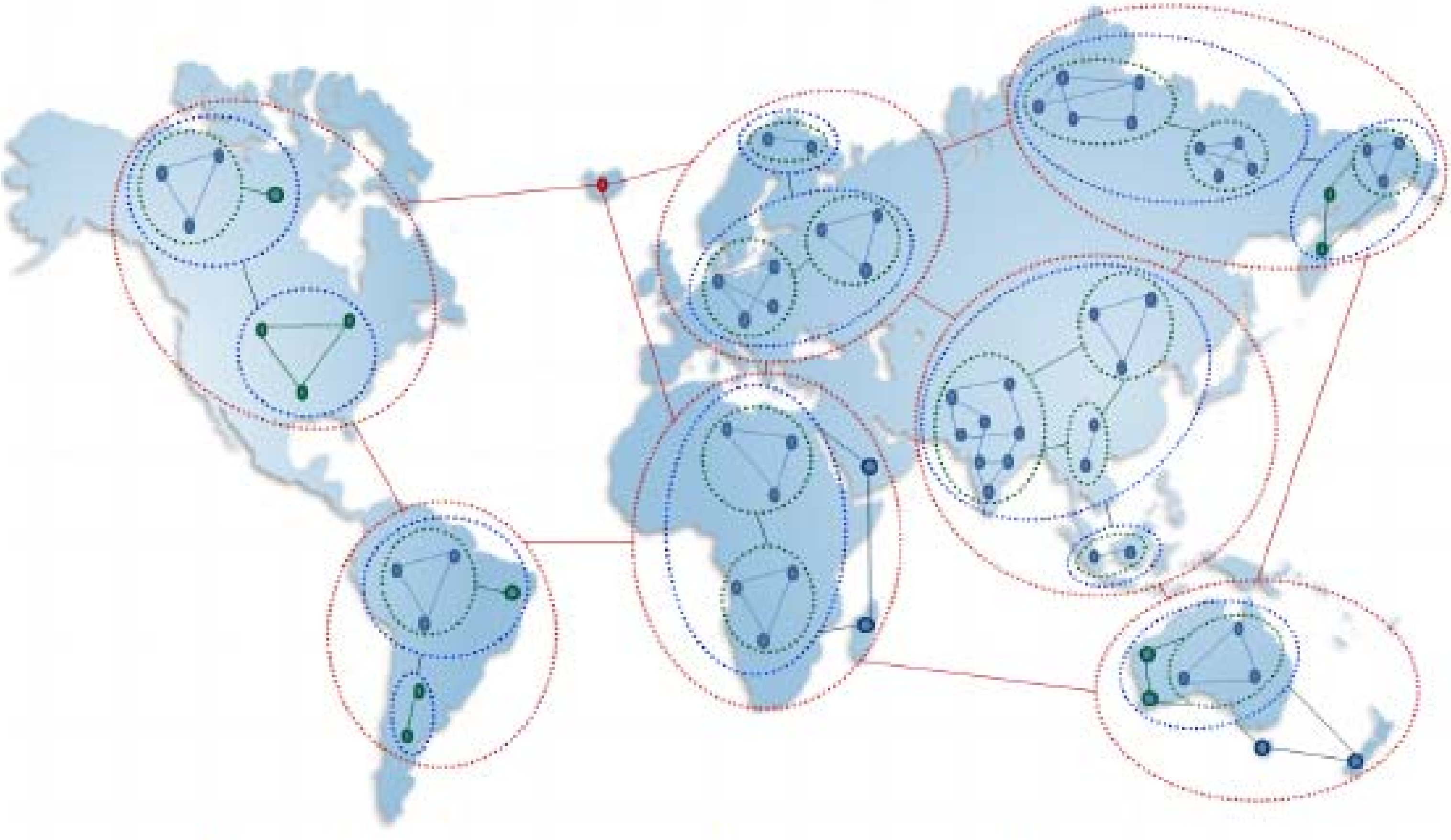


Figure 1. Decentralized network views at various levels of hierarchy.

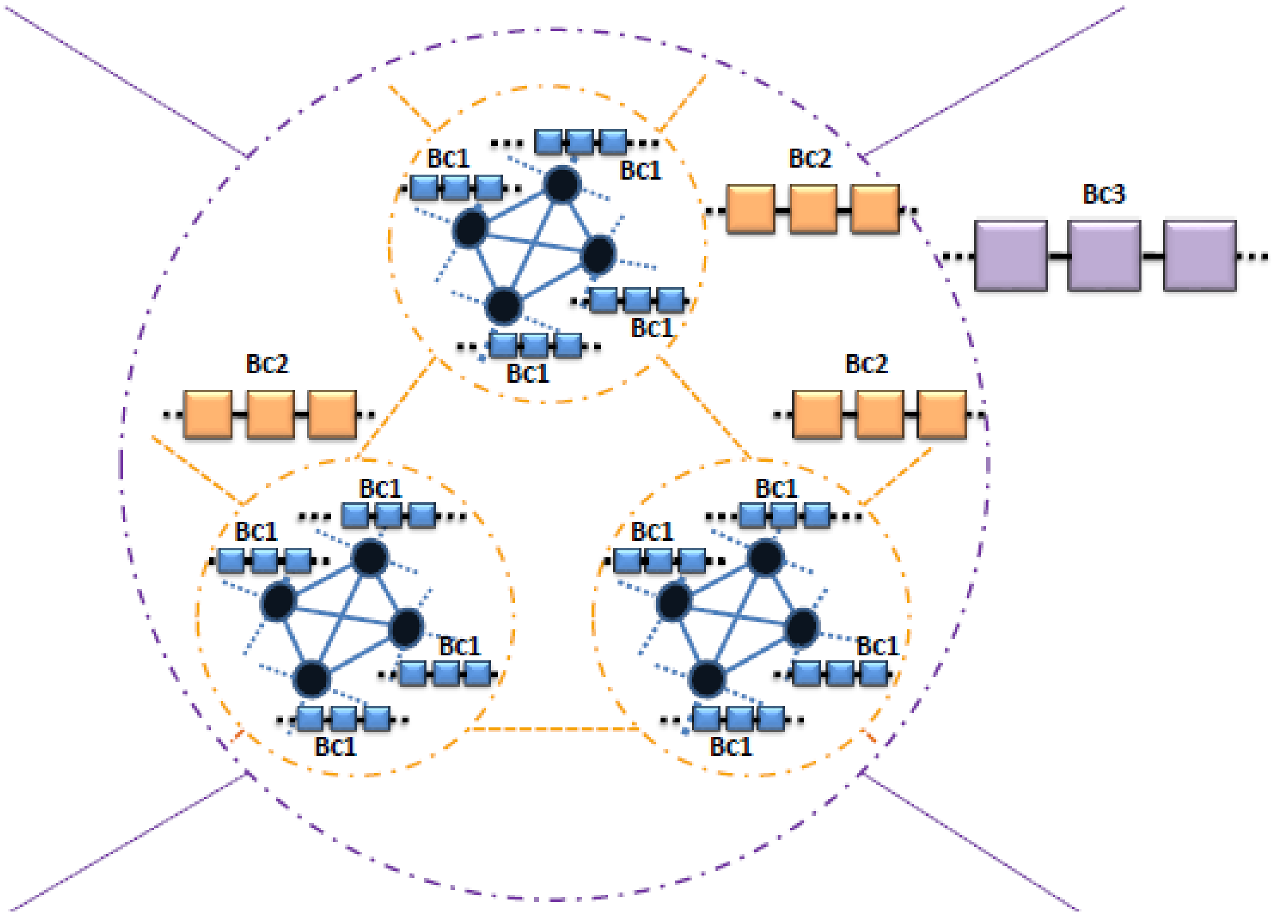


Figure 2. Schematic diagram of hierarchical blockchains model.

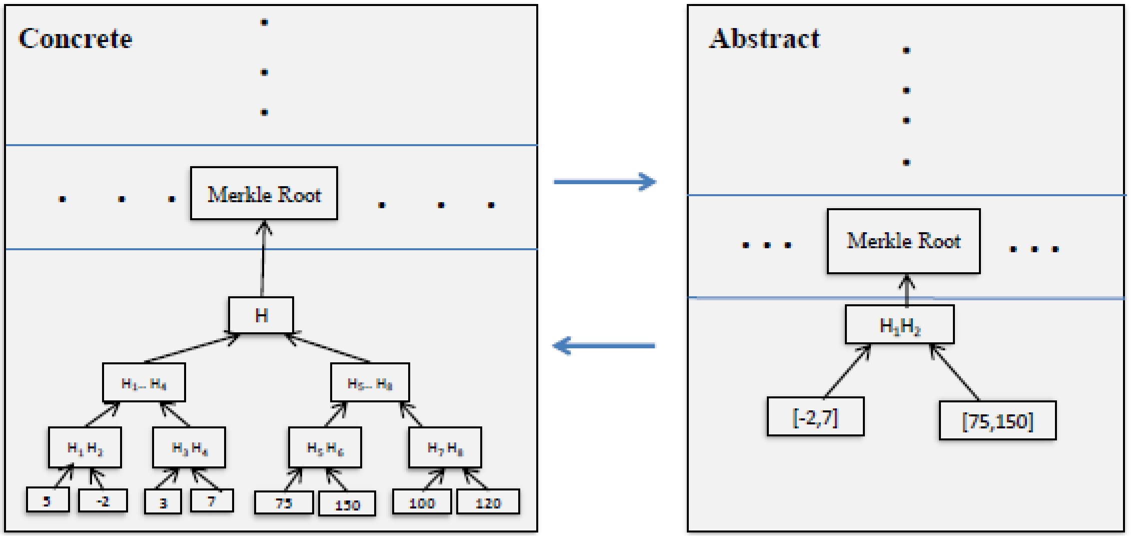


Figure 8. Abstract Block in Interval Domain.

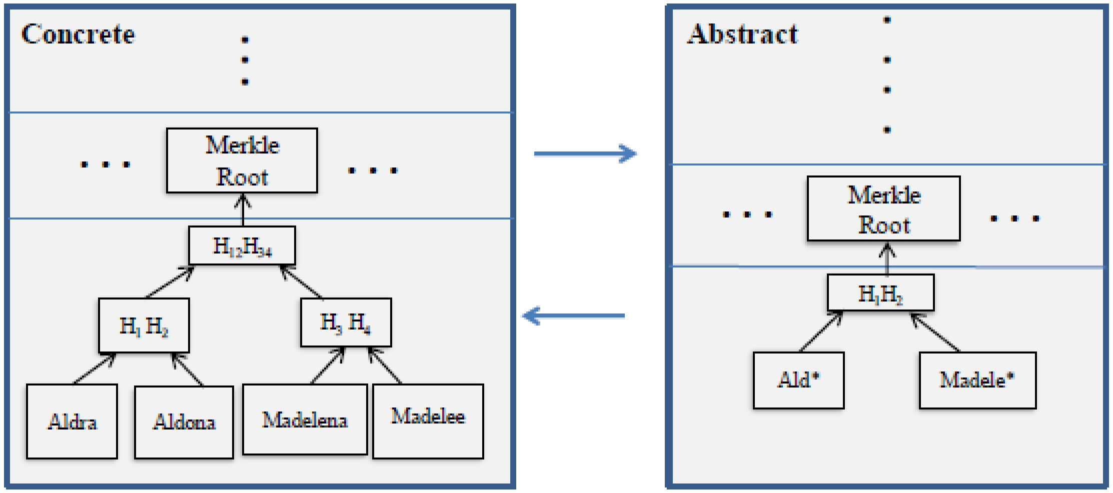
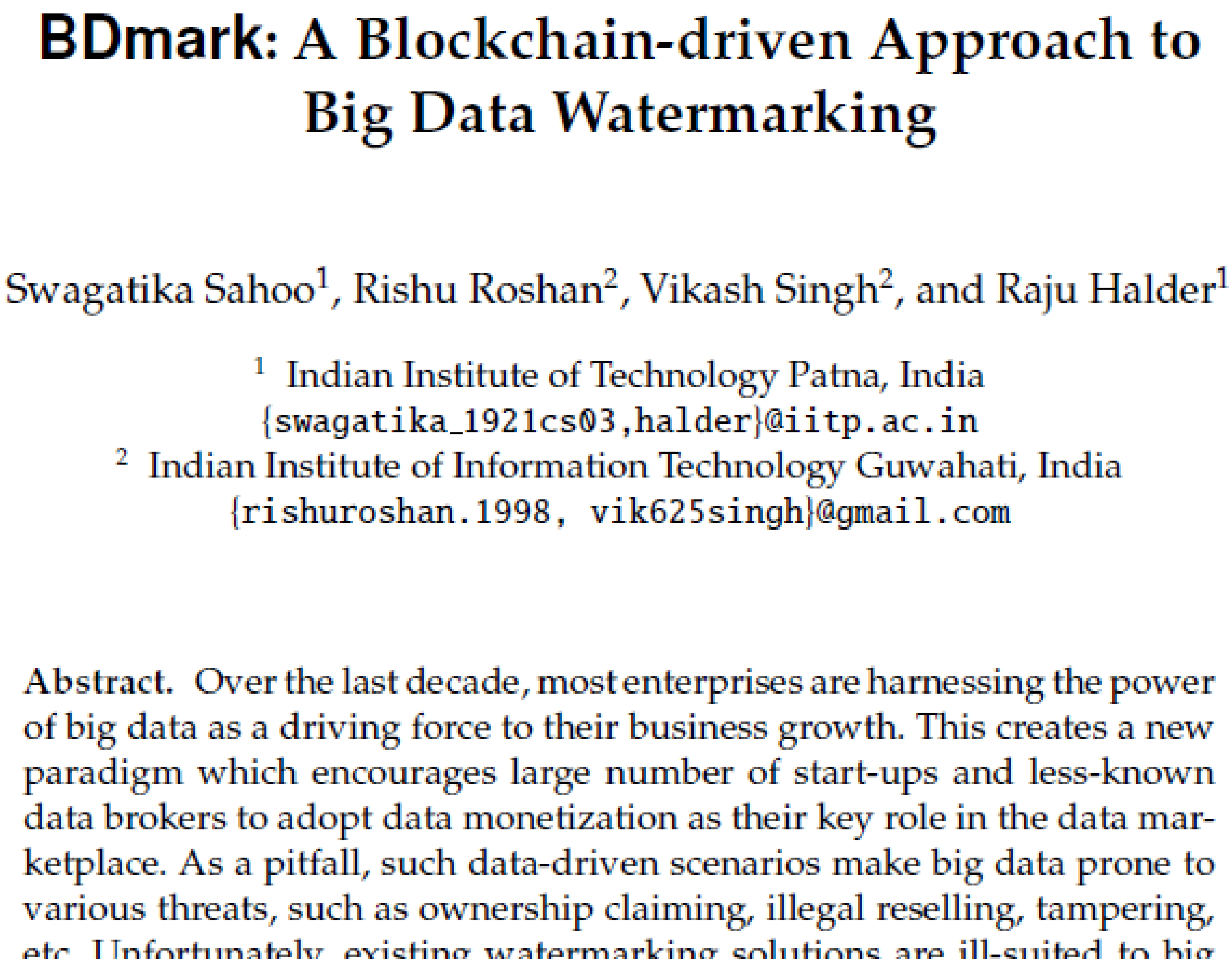


Figure 9. Abstract Block in Prefix Domain.



BDmark: A Blockchain-driven Approach to Big Data Watermarking

Swagatika Sahoo[1], Rishu Roshan[2], Vikash Singh[2], and Raju Halder[1]

[1] Indian Institute of Technology Patna, India
{swagatika_1921cs03,halder}@iitp.ac.in
[2] 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

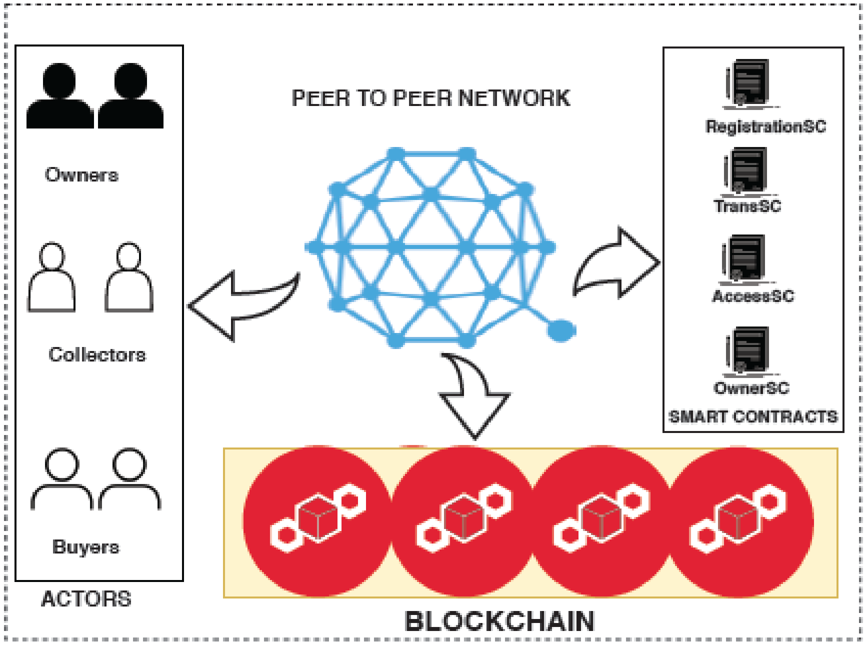


Fig. 1: **A pictorial representation of the overall system components**

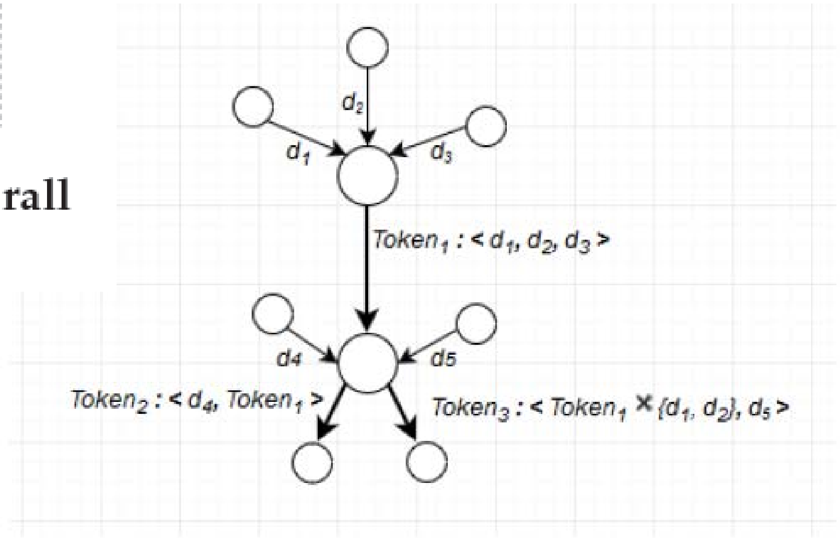

d_2
d_1
d_3
$Token_1 : < d_1, d_2, d_3 >$
$d4$
$d5$
$Token_2 : < d_4, Token_1 >$
$Token_3 : < Token_1 \times \{d_1, d_2\}, d_5 >$

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

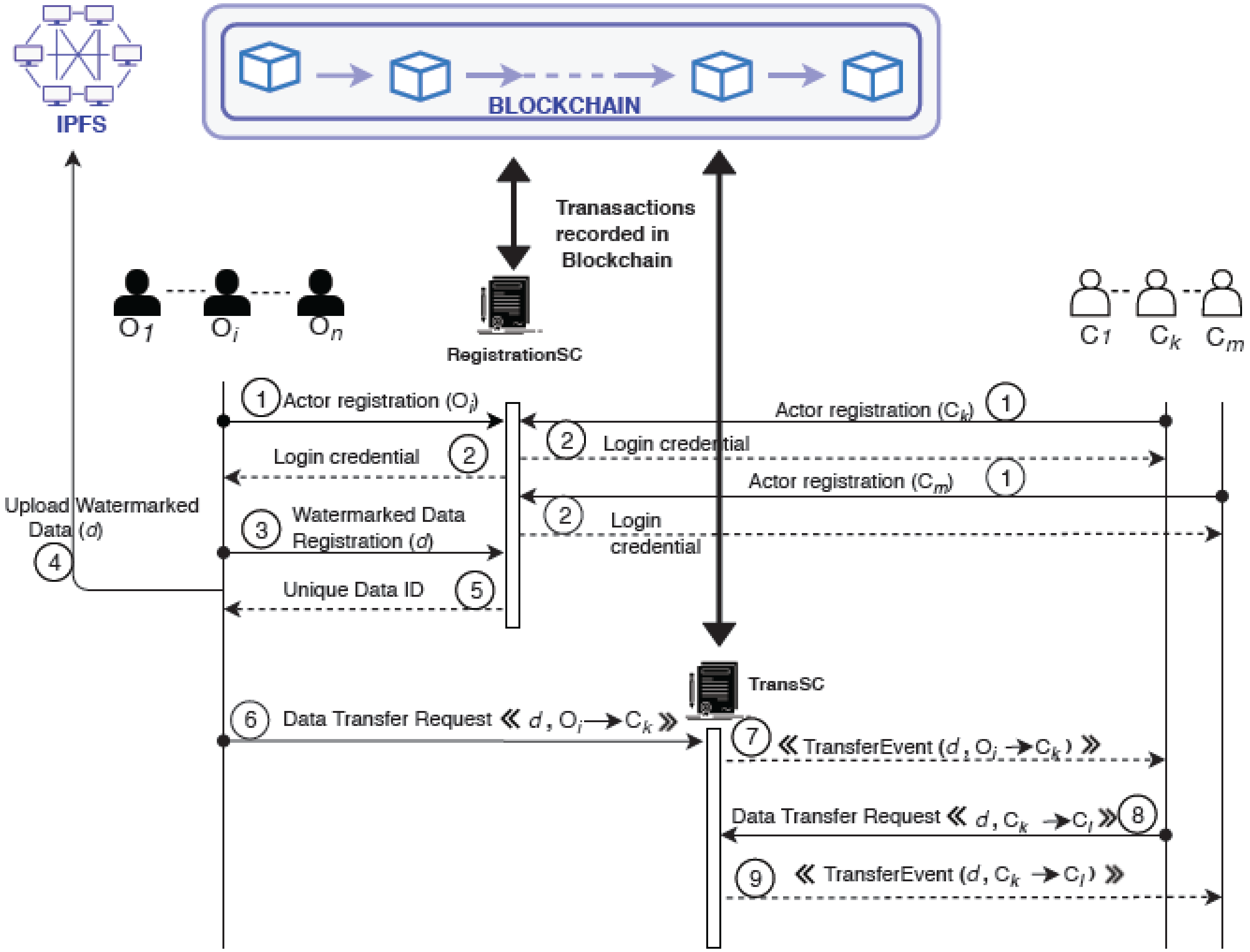

IPFS
BLOCKCHAIN
Tranasactions recorded in Blockchain
O1
Oi
On
RegistrationSC
C1
Ck
Cm
1 Actor registration (Oi)
2 Login credential
Upload Watermarked Data (d)
4
3 Watermarked Data Registration (d)
Unique Data ID 5
Actor registration (Ck) 1
2 Login credential
Actor registration (Cm) 1
2 Login credential
TransSC
6 Data Transfer Request « d , Oi ⟶ Ck »
7 « TransferEvent (d , Oi ⟶ Ck) »
Data Transfer Request « d , Ck ⟶ Cl » 8
9 « TransferEvent (d , Ck ⟶ Cl) »

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

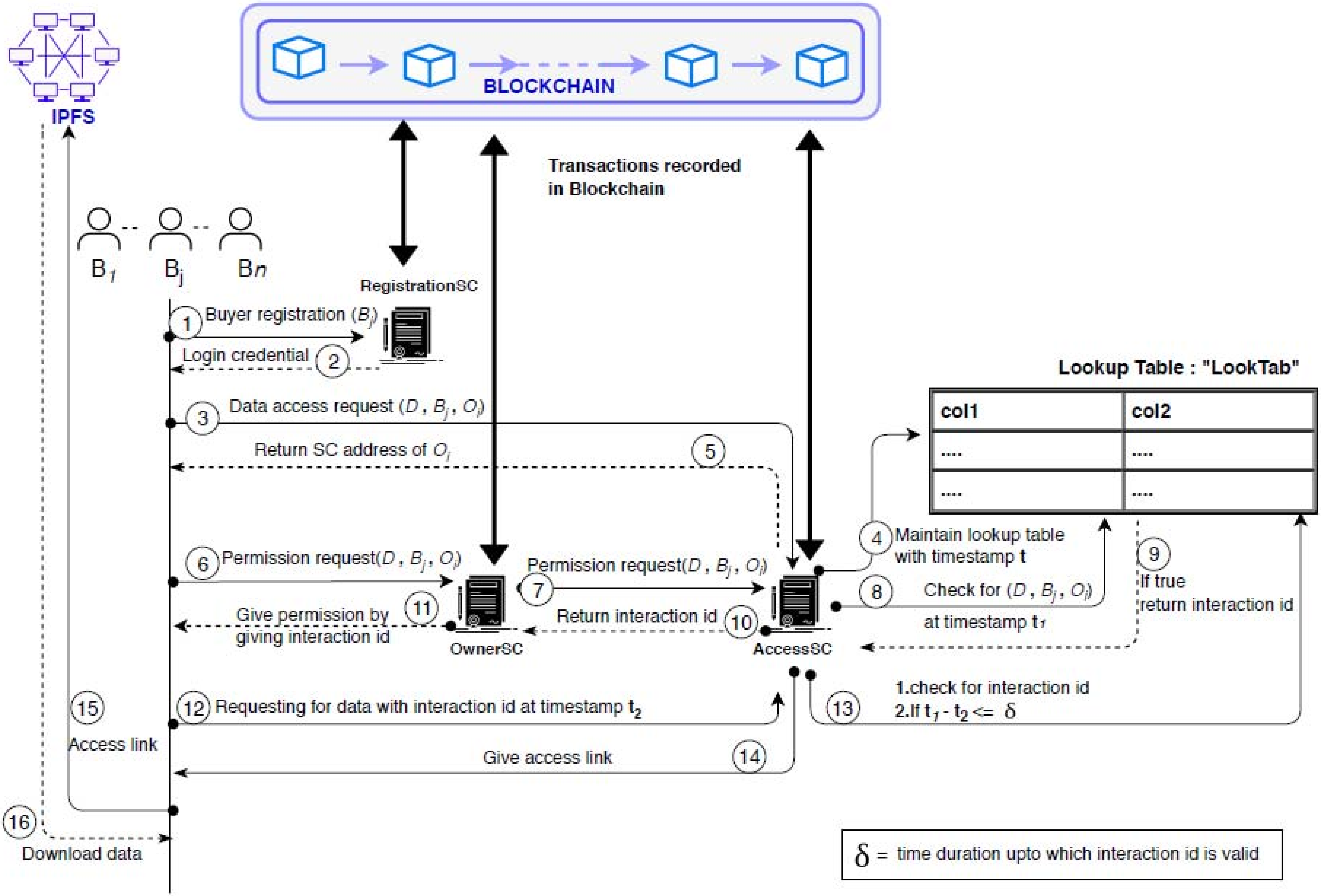
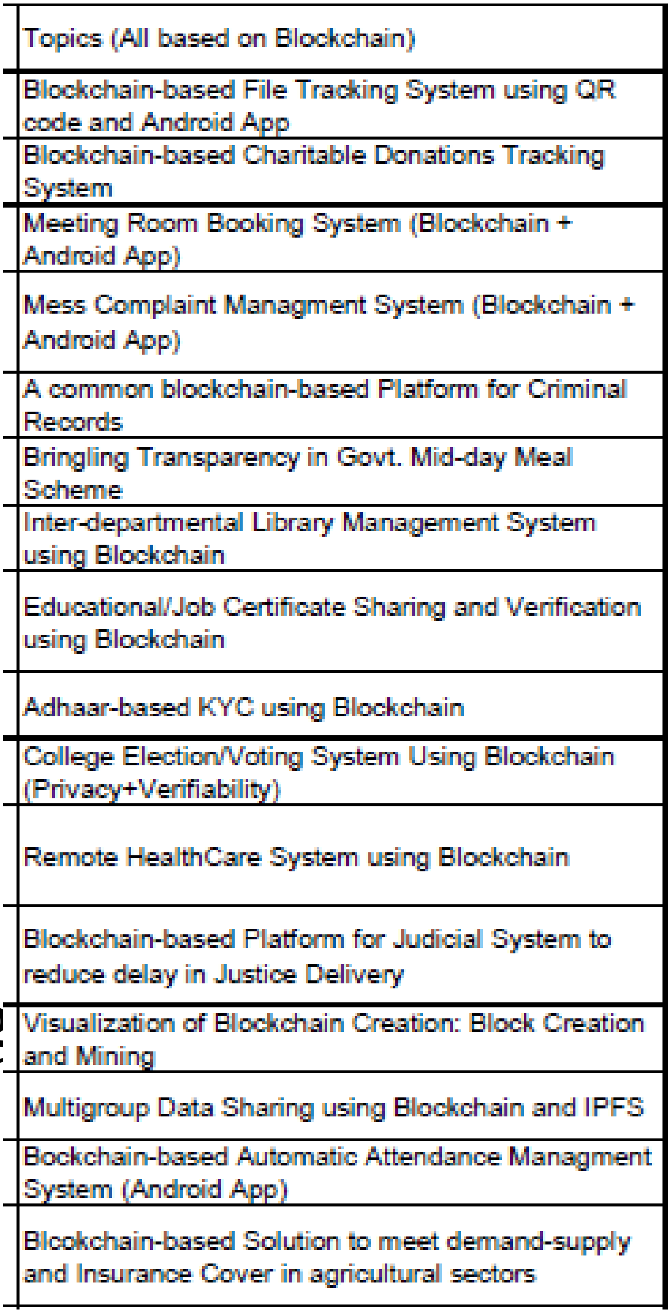

IPFS
BLOCKCHAIN
Transactions recorded in Blockchain
B_1
B_j
B_n
RegistrationSC
1 Buyer registration (B_j)
Login credential 2
3 Data access request (D , B_j , O_j)
Return SC address of O_j
5
Lookup Table : "LookTab"
col1
col2
....
....
....
....
4 Maintain lookup table with timestamp t
6 Permission request(D , B_j , O_j)
Permission request(D , B_j , O_j)
7
8 Check for (D , B_j , O_j) at timestamp t_1
9 If true return interaction id
Give permission by giving interaction id
11
OwnerSC
Return interaction id
10
AccessSC
15
Access link
12 Requesting for data with interaction id at timestamp t_2
13
1.check for interaction id
2.If t_1 - t_2 <= δ
Give access link
14
16
Download data
δ = time duration upto which interaction id is valid

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

More!

- Asset Transafer
- 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 Managment System (Blockchain + Android App)
A common blockchain-based Platform for Criminal Records
Bringling 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
Bockchain-based Automatic Attendance Managment System (Android App)
Blcokchain-based Solution to meet demand-supply and Insurance Cover in agricultural sectors