Distributed Ledger Technology for Trust Management Optimisation in M2M

24. ITG-Fachtagung Mobilkommunikation

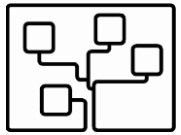
Besfort Shala

shala@e-technik.org

Frankfurt University of Applied Sciences, Germany
Research Group for Telecommunication Networks

FRANKFURT UNIVERSITY OF APPLIED SCIENCES

Kleiststraße 3, D-60318 Frankfurt a.M.
E-Mail: shala@e-technik.org



Outline

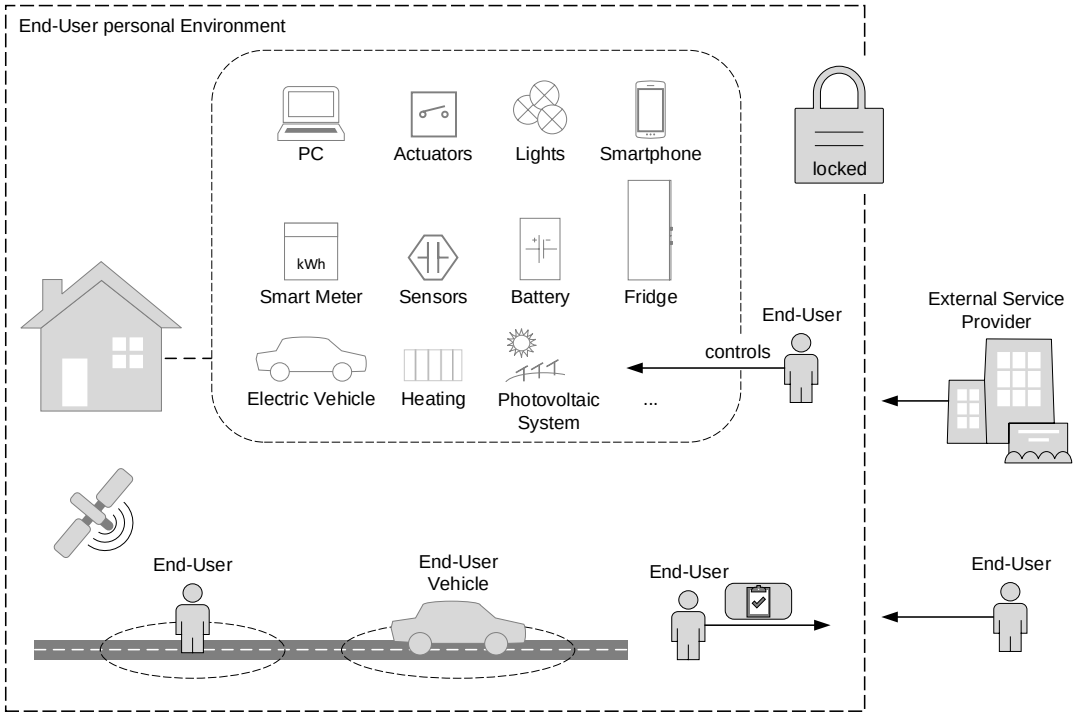
1. Decentralised M2M Application Service
2. Trust Management and Evaluation Approaches
3. Distributed Ledger Technology
4. M2M Trust Evaluation System
5. Conclusion

1 Decentralised M2M Application Service

Intelligent devices in end-user environment (devices provide monitoring, controlling and communication functionality)

Various M2M application fields:

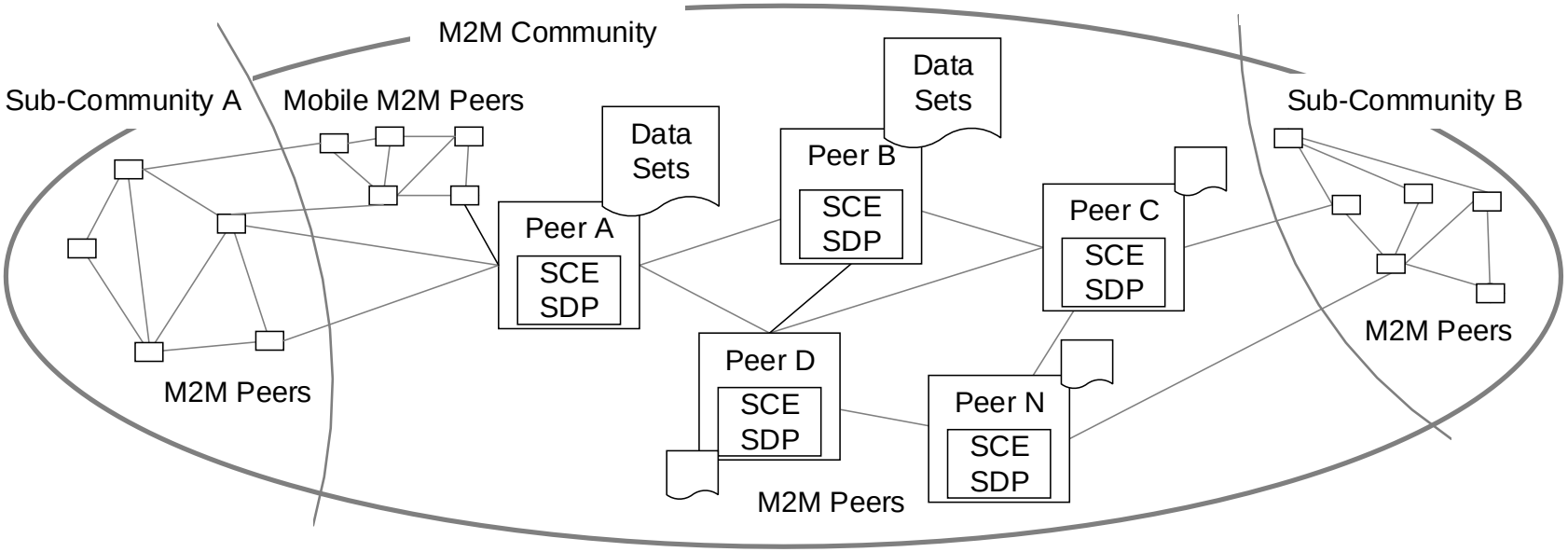
- **Energy management**
- **Building surveillance**
- **Smart home**



Limitations of existing M2M service platforms:

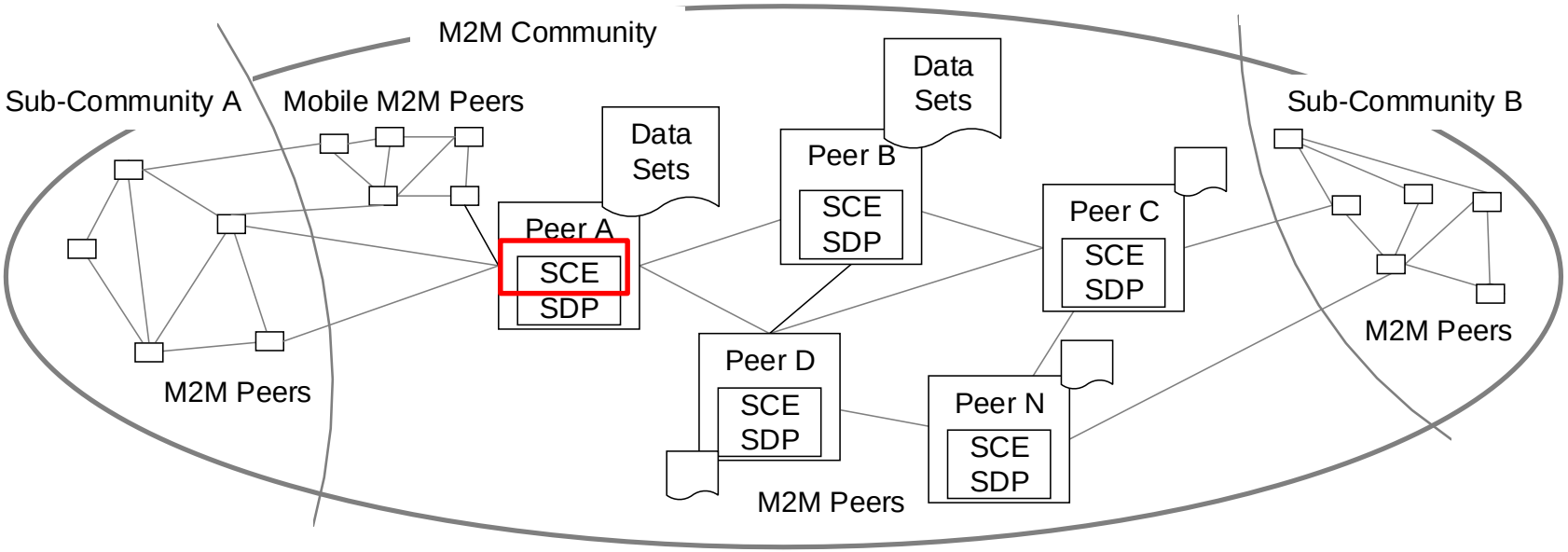
- **Expert knowledge required** (not applicable by end-users)
- **Central stakeholders or infrastructure elements** (dependencies, costs,…)

Decentralised M2M Application Service 2



- **Services are realised by one ore more peers**
- **Application is a combination of one or more underlying services**

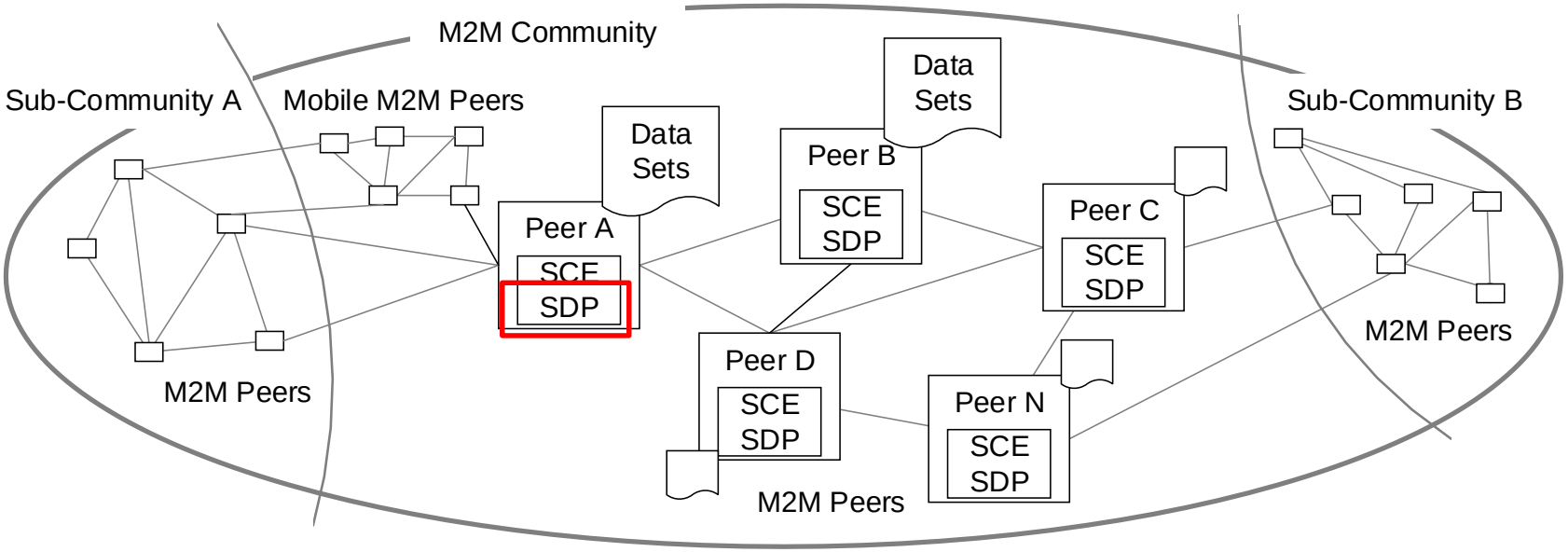
Decentralised M2M Application Service 3



Service Creation Environment (local)**:**

- **End-users develop individual M2M applications**
- **M2M applications integrate M2M resources and multimedia communication**

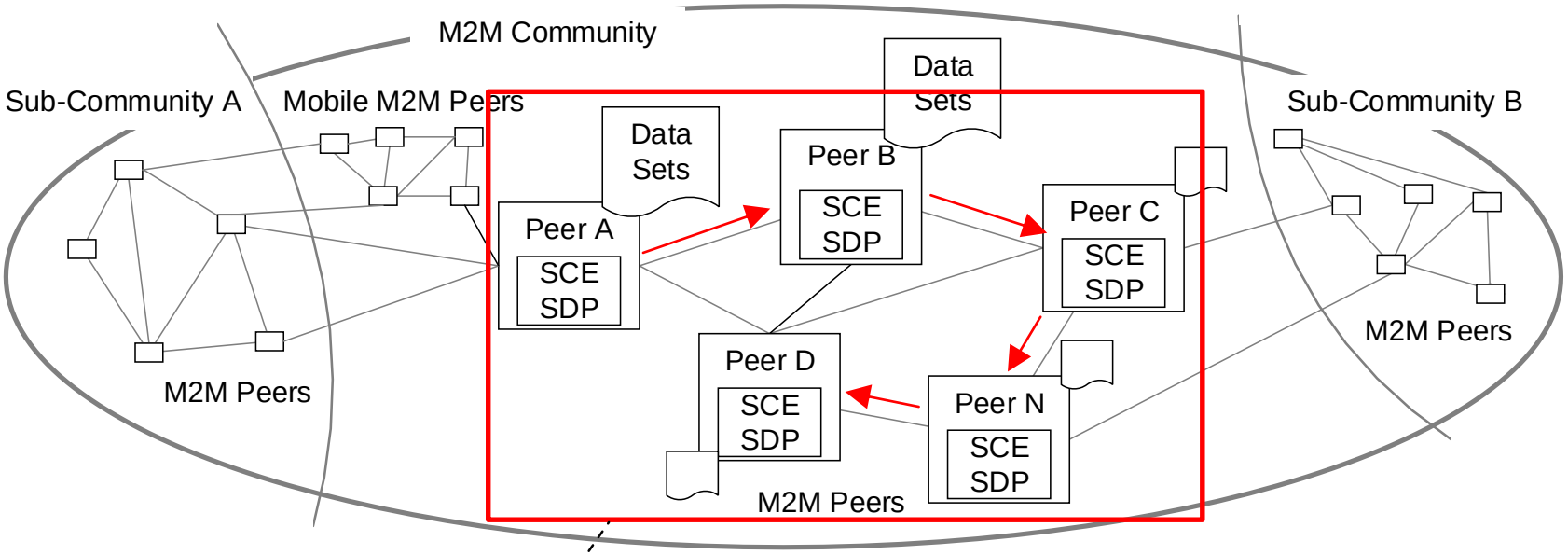
Decentralised M2M Application Service 4



Service Delivery Platform (local)**:**

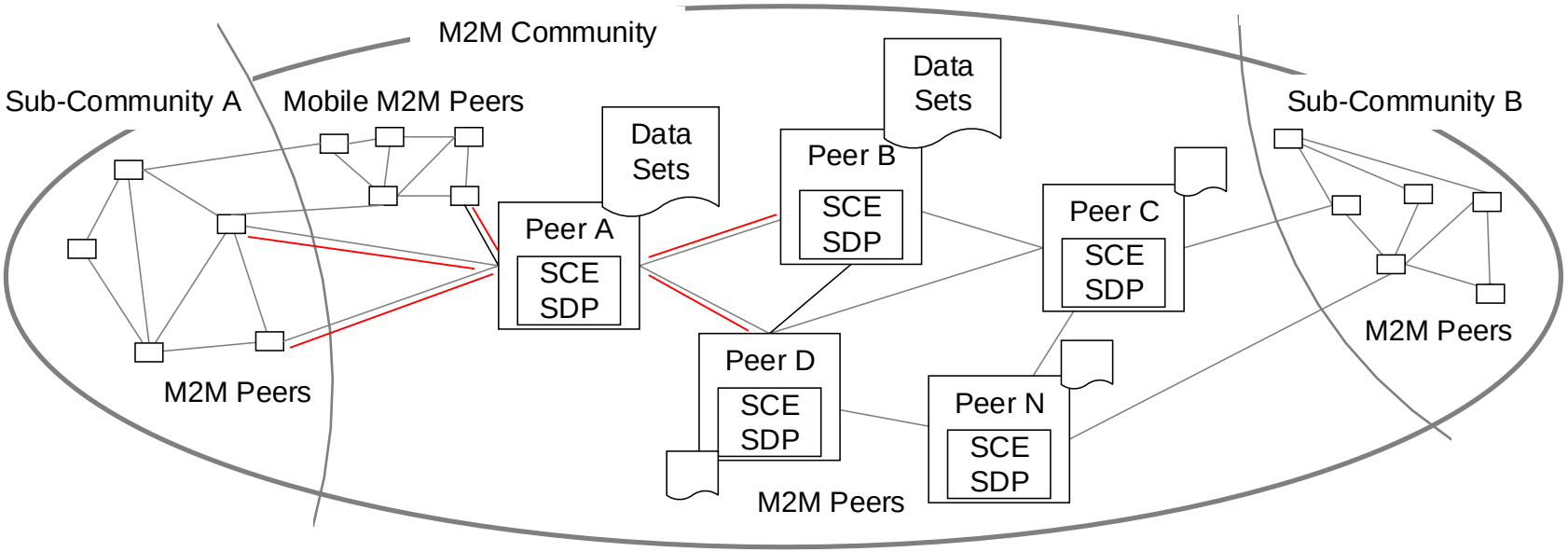
- **Executes M2M applications**

Decentralised M2M Application Service



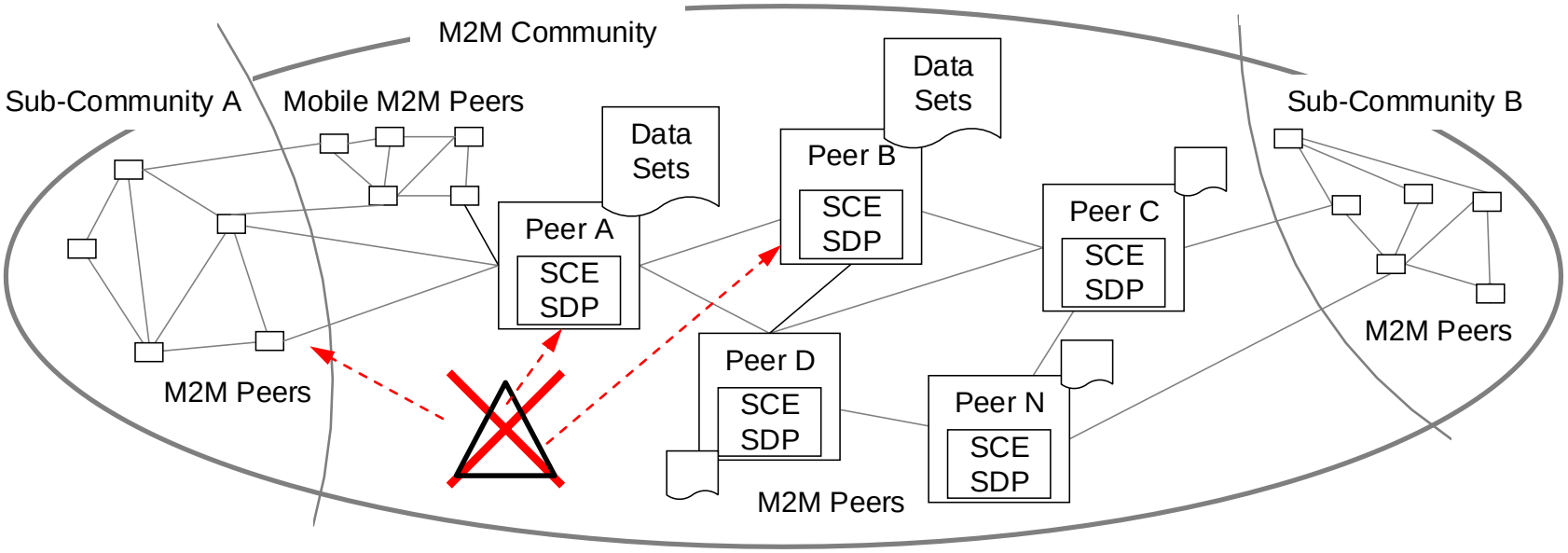
Peers link local services to provide a cooperative/distributed M2M application

Decentralised M2M Application Service 6



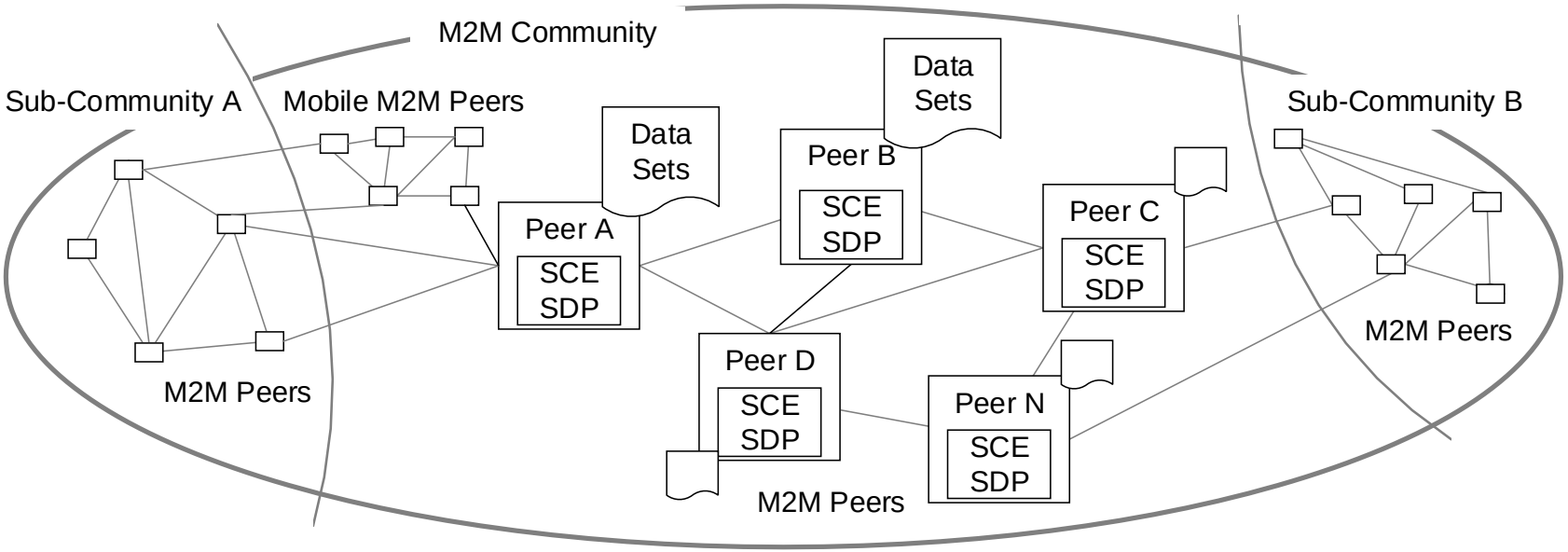
P2P communication between service provider and service consumer (no intermediary entities)

Decentralised M2M Application Service



M2M system architecture contains no central entities(e.g. central platform elements, stakeholders)

Decentralised M2M Application Service 8



M2M community:

- **Social M2M network** (for M2M services)
- **Uniform platform to connect participants**
- **Sub-communities form interest groups**

Decentralised M2M Application Service 9

Limitations:

- **End-user with less technical knowledge**
  → wrong or malfunctioning services

- **Untrustworthy peers**
  → malfunctioning or malicious services

- **Joining/leaving peers or services**
  → breaking down the network or application

- **Random selection of services**
  → unsecure or untrusted service providers

2 Trust Management and Evaluation Approaches

Prevent security problems:

- **Trust relationships between the peers**

How to establish trust relationships?

1. **Define how the trust score of a peer is computed**
2. **Define which parameters are considered for the trust evaluation**
3. **Define who is going to do the trust evaluation**
4. **Define how the computed trust scores are managed.**

Trust Management and Evaluation Approaches 2

- **Several existing trust approaches in M2M and in other related fields** (P2P systems)

Trust Management Approaches	Requirements				
	Decentralised Evaluation	Initial Trust Score	Ongoing Trust Score	Tamper-proof Storage	Comprehensive Trust Model
DisTMIoT	+	-	+	o	-
RecomTrust	o	o	+	-	-
TaHCIoT	o	-	+	-	-
TMSD	-	-	+	-	-
PSIoTrust	-	o	-	-	-
TruClust	o	-	+	-	o
TBootSP	+	o	-	-	-
ReputaBoot	+	o	-	-	o
TrustSSC	-	-	+	-	o

Legend: + satisfied; - not satisfied; o partially satisfied

Trust Management and Evaluation Approaches 3

Trust Management Approaches	Requirements				
	Decentralised Evaluation	Initial Trust Score	Ongoing Trust Score	Tamper-proof Storage	Comprehensive Trust Model
DisTMIoT	+	-	+	o	-
RecomTrust	o	o	+	-	-
TaHCIoT	o	-	+	-	-
TMSD	-	-	+	-	-
PSIoTrust	-	o	-	-	-
TruClust	o	-	+	-	o
TBootSP	+	o	-	-	-
ReputaBoot	+	o	-	-	o
TrustSSC	-	-	+	-	o

Legend: + satisfied; - not satisfied; o partially satisfied

3 Distributed Ledger Technology

Basics:

- **An asset database that can be shared across a network of multiple sites, geographies or institutions**
- **All participants can have their own identical copy of the ledger.**
- **Any changes to ledger are reflected in all copies**
- **Security and accuray of assets stored in the ledger are maintained cryptographically**
- **Two architectures used in distributed ledger approaches:**
  - **Blockchain**
  - **Directed Acyclic Graph**

Advantages of using Blockchain:

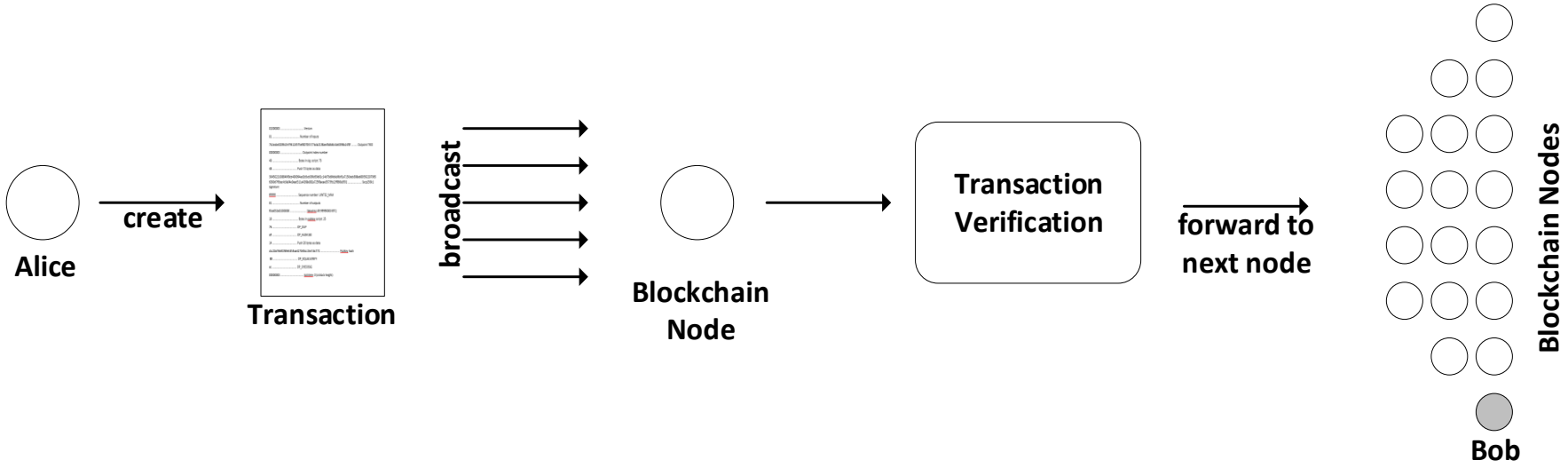
- **decentralization,**
- **transparency**
- **immutability**

Example for using blockchain to store transactions – Bitcoin

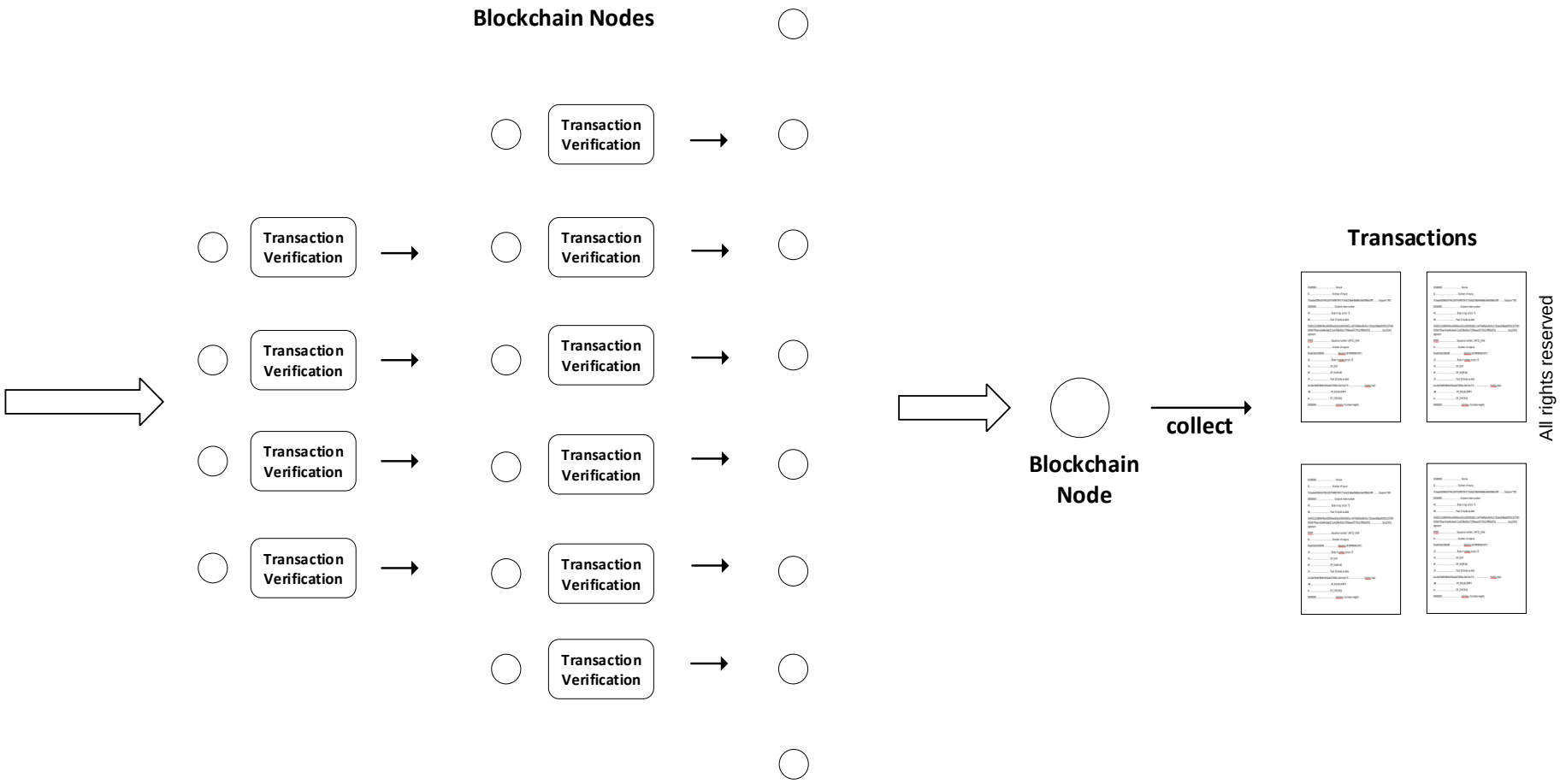
Five key components of a blockchain

1. **Cryptography**
2. **P2P network**
3. **Consensus mechanism**
4. **Ledger**
5. **Validity rules**

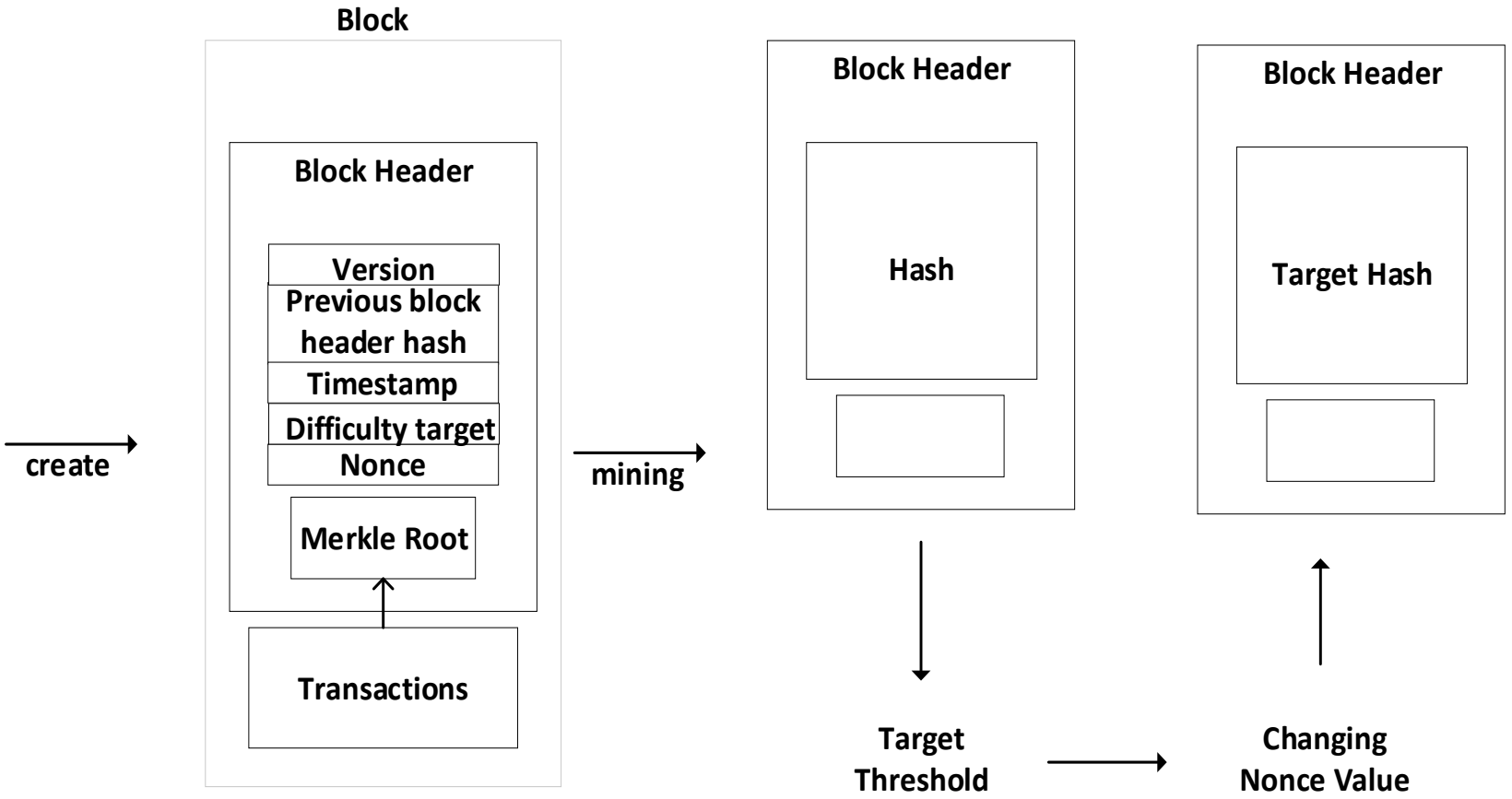
Alice sending a transaction to Bob



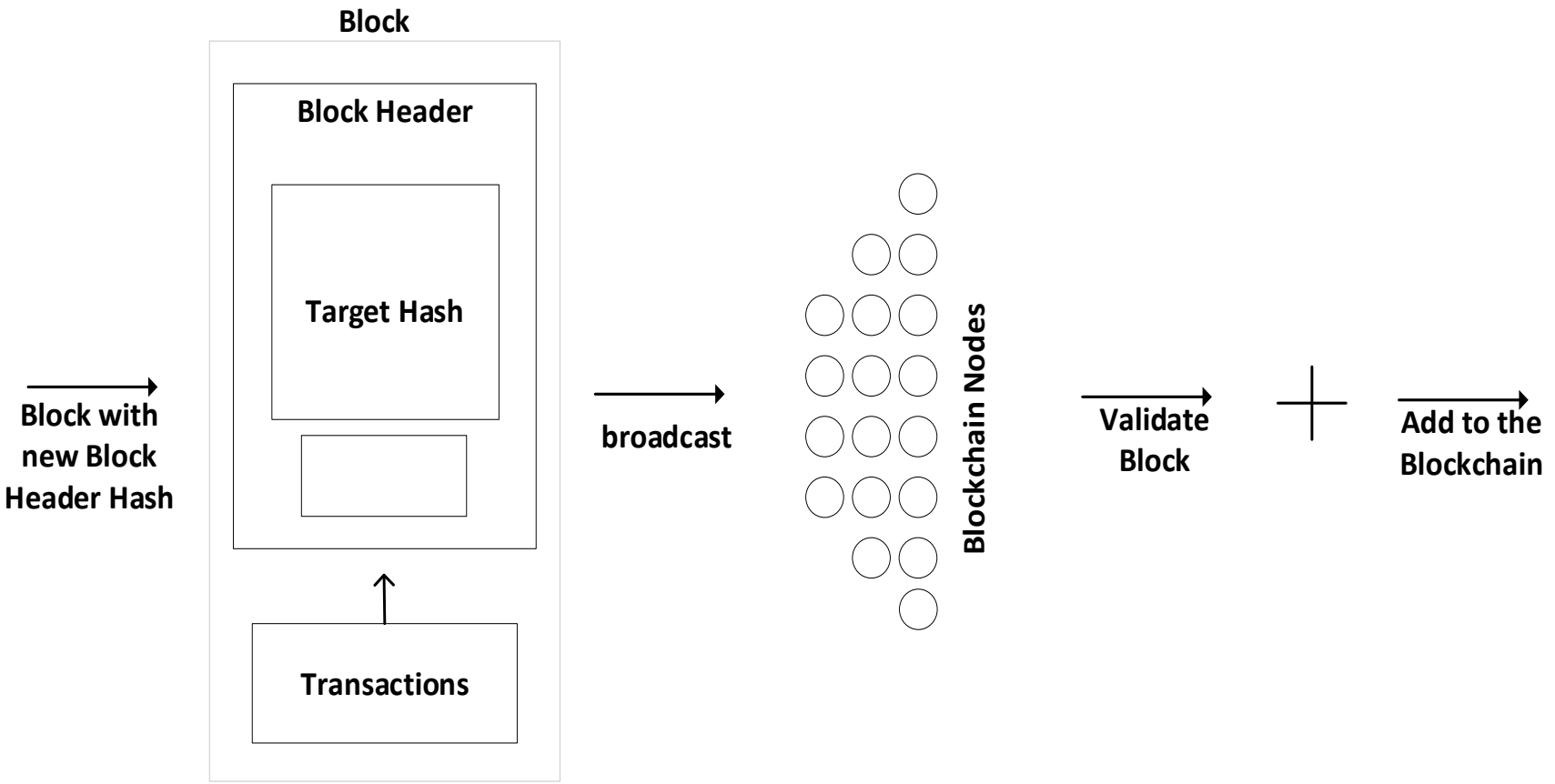
Transaction forwarding and collection



Block creation and mining



Block validation and integration



- **Five key components of a blockchain**
  1. **Cryptography**
  2. **P2P network**
  3. **Consensus mechanism**
  4. **Ledger**
  5. **Validity rules**

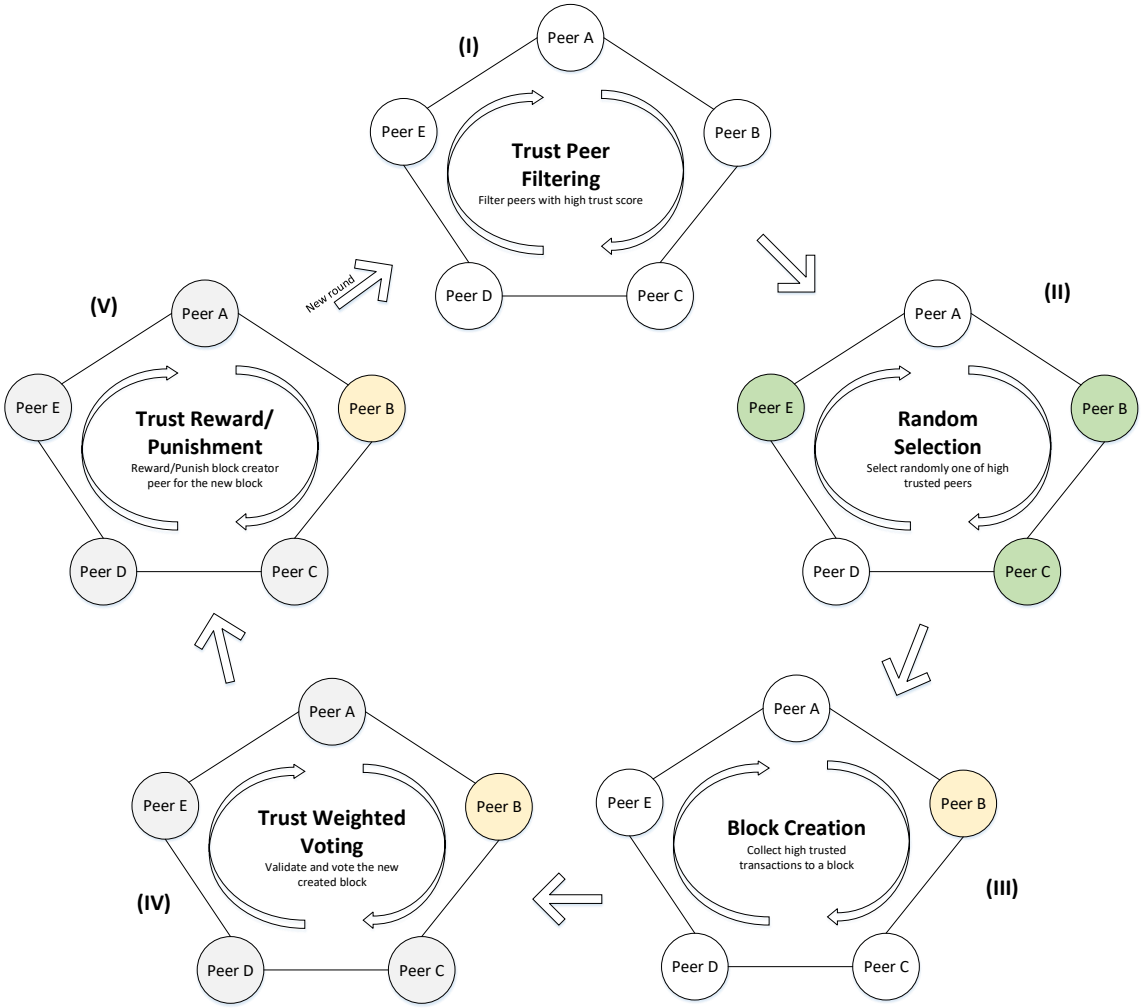
- **Consensus between the nodes to agree for the same copy of the ledger**
- **Consensus mechanism is a set of steps taken by the participating nodes to agree on a proposed state.**

Review of existing consensus mechanisms

Consensus mechanism	Computational Effort	Trusted Block Creator Selection	Trusted Block Creation	Trusted Transaction	Decentralized Architecture	Trust Reward/Punishment	Resilient Against Fake Transaction Attacks	Reliable Validation Decision Process
PoW	-	o	-	-	+	o	o	-
PoS	o	o	-	-	o	-	-	-
DPoS	o	o	-	-	o	-	-	-
Nano	o	o	-	-	o	-	-	-
Ripple	+	n/a	o	-	o	-	o	o
Tangle	o	-	o	o	o	-	o	-

Legend: + satisfied; - not satisfied; o partially satisfied

- **Proposed „Proof of Trust“ consensus mechanism**



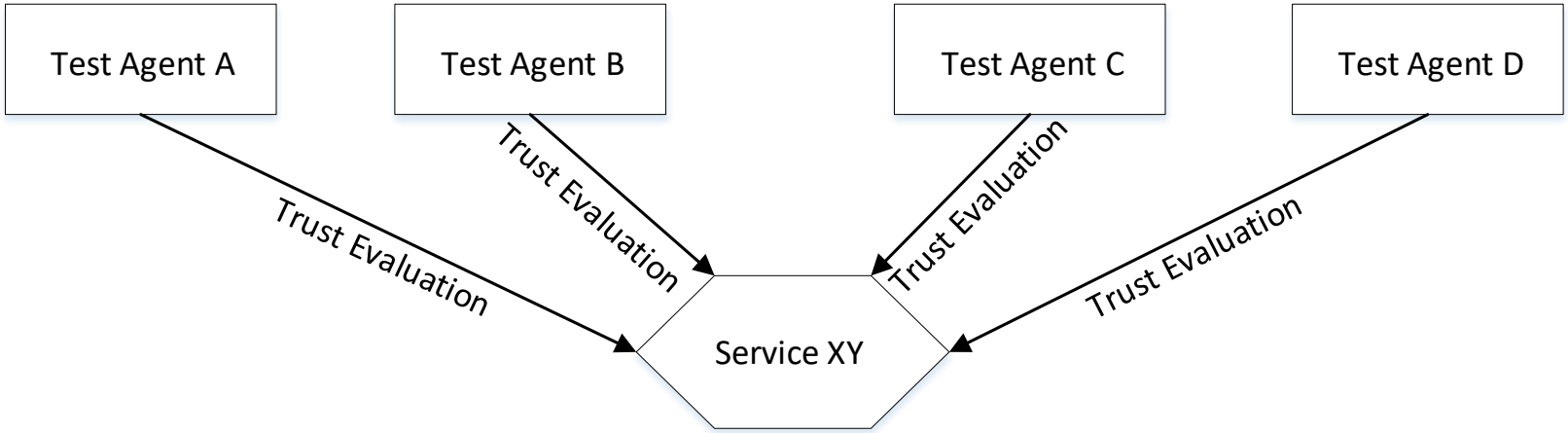
5 M2M Trust Evaluation System

Identified problems in existing trust evaluation systems:

1. **Decentralised Architecture**
2. **Data Storage**
3. **Initial Trust Score**
4. **Comprehensive Trust Model**

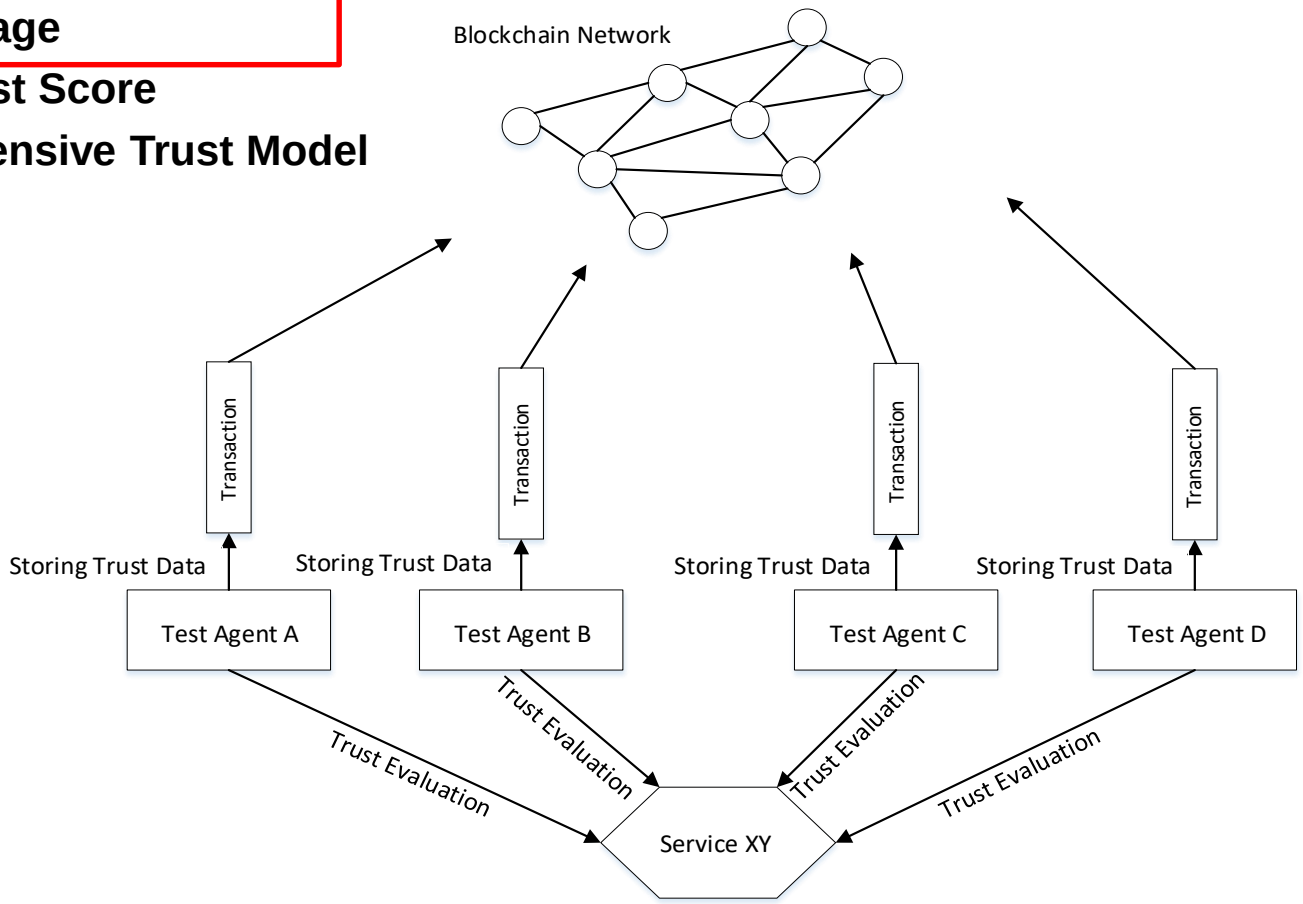
→ Other peers act as Test Agents

→ Share their evaluation results in the P2P network

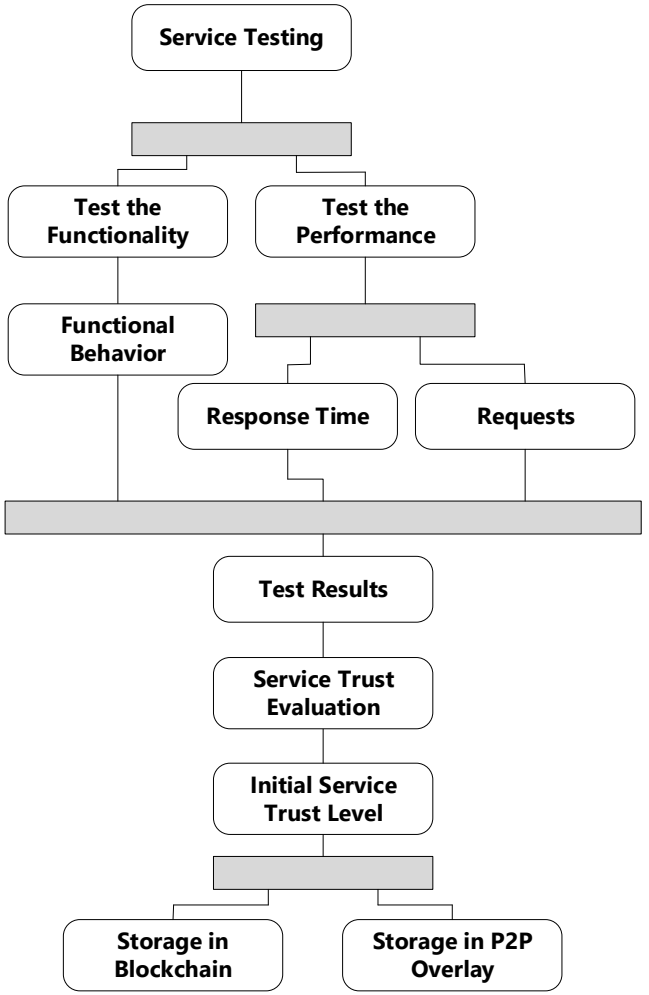


M2M Trust Evaluation System 2

- **Identified problems in existing trust evaluation systems:**
  1. **Decentralised Architecture**
  2. **Data Storage**
  3. **Initial Trust Score**
  4. **Comprehensive Trust Model**

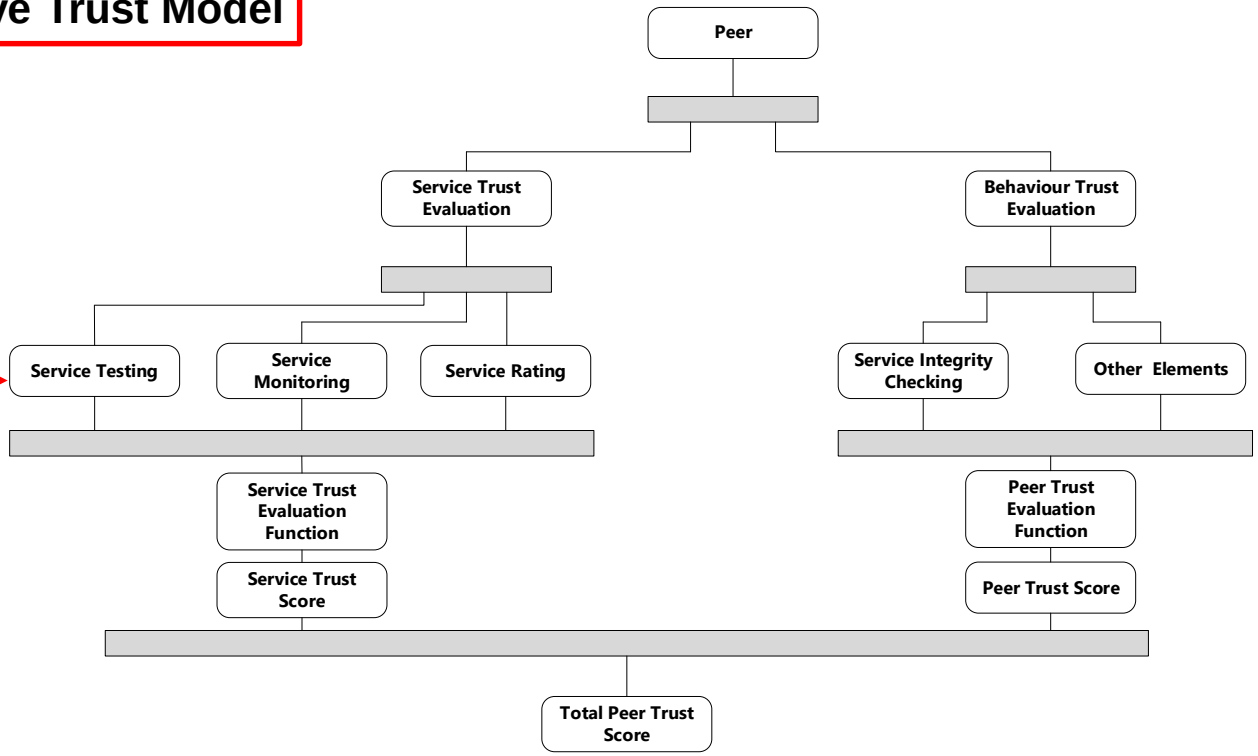


- **Identified problems in existing trust evaluation systems:**
  1. **Decentralised Architecture**
  2. **Data Storage**
  3. **Initial Trust Score**
  4. **Comprehensive Trust Model**



M2M Trust Evaluation System

- **Identified problems in existing trust evaluation systems:**
  1. **Decentralised Architecture**
  2. **Data Storage**
  3. **Initial Trust Score**
  4. **Comprehensive Trust Model**



5 Conclusion

- **Limitations of existing trust approaches**
- **Limitations of existing consensus mechanisms**
- **New consensus mechanism**
- **Integration of blockchain for framework optimisation**
- **Comprehensive trust evaluation system**

Distributed Ledger Technology for Trust Management Optimisation in M2M

24. ITG-Fachtagung Mobilkommunikation

Besfort Shala

shala@e-technik.org

Frankfurt University of Applied Sciences, Germany
Research Group for Telecommunication Networks

FRANKFURT UNIVERSITY OF APPLIED SCIENCES

Kleiststraße 3, D-60318 Frankfurt a.M.
E-Mail: shala@e-technik.org