UNIVERSITAS
GADJAH MADA

Blockchain: Beyond Cryptocurrencies

Dr. Guntur D Putra

Presented at
The 2024 8th International Conference on Information Technology, Information Systems and Electrical Engineering (ICITISEE)
Grand Keisha Yogyakarta, Indonesia

Guntur Dharma Putra

gdputra@ugm.ac.id

Education

Electrical Engineering
Universitas Gadjah Mada, Indonesia — B.Eng. (2014)

Information Science
Saga University, Japan — Non-Degree (2012)

Computing Science
University of Groningen, the Netherlands — M.Sc. (2017)

Computer Science and Engineering
UNSW, Australia — Ph.D. (2022)

Affiliation
Assistant Professor
Department of Electrical and Information Engineering
UGM

Area of research
Distributed Systems
Security and Privacy
Blockchain
Internet of Things

Online Profile

GitHub gtrdp
LinkedIn guntur-dharma-putra
Google Scholar user=L_dr0dIAAAAJ
https://gdputra.github.io

Guntur Dharma Putra

gdputra@ugm.ac.id

Community Service

Membership

Member, Institute of Electrical and Electronics Engineers (IEEE)
Member, IEEE Communications Society
Member, IEEE Computer Society
Member, Association for Computing Machinery (ACM)
Member, The Institution of Engineers Indonesia (PII)

Service

Conferences:

2024: IEEE PerCom, IEEE ICBC, IEEE Blockchain, IEEE Metacom
2023: IEEE MetaCom, ICBC, IEEE Blockchain
2022: ICBC, INFOCOM, Blockchain
2021: ICDCS, ICBC, IEEE MASS, BRAINS, LCN, ISCC
2020: IEEE DAPPS, ICBC, ICC

Journals:

Elsevier - Pervasive and Mobile Computing
Elsevier - Journal of Information Security and Applications
Elsevier - Ad Hoc Networks
Elsevier - Applied Ergonomics
Elsevier - Computer Communications
Elsevier - Computer Networks
IEEE Transactions on Network and Service Managements
IEEE Computer Magazine
IEEE Transactions on Vehicular Technology
IEEE Internet of Things Journal
IEEE Internet of Things Magazine
IEEE Access
IEEE Security and Privacy
ACM Transactions on Internet of Things

What is Blockchain?

"A **blockchain** is a ***growing list of records***, called *blocks*, that are *linked together using cryptography*. Each block contains a cryptographic *hash of the previous block*, a timestamp, and transaction data."

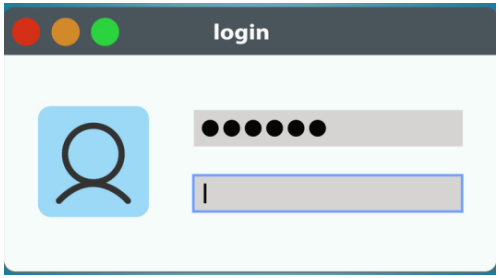
–Wikipedia

What My Talk is All About

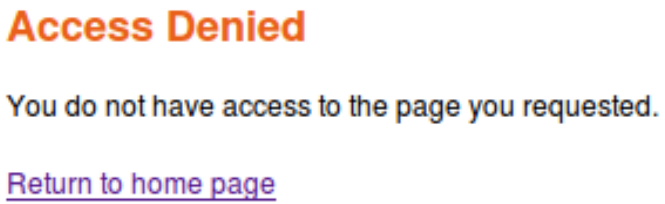
- Securing the Internet of Things
- Interoperable Self-Sovereign Identity

IoT Access Control

Authentication and Authorization



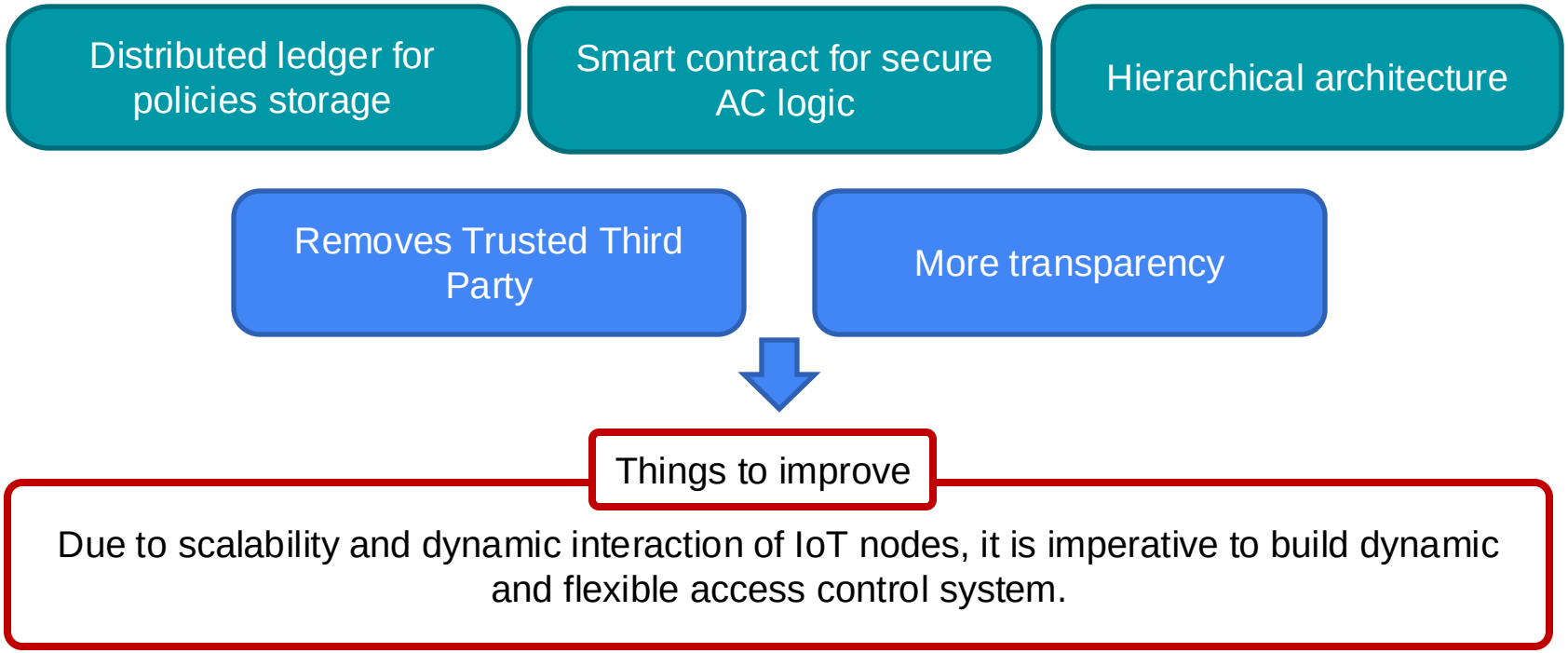
Authentication



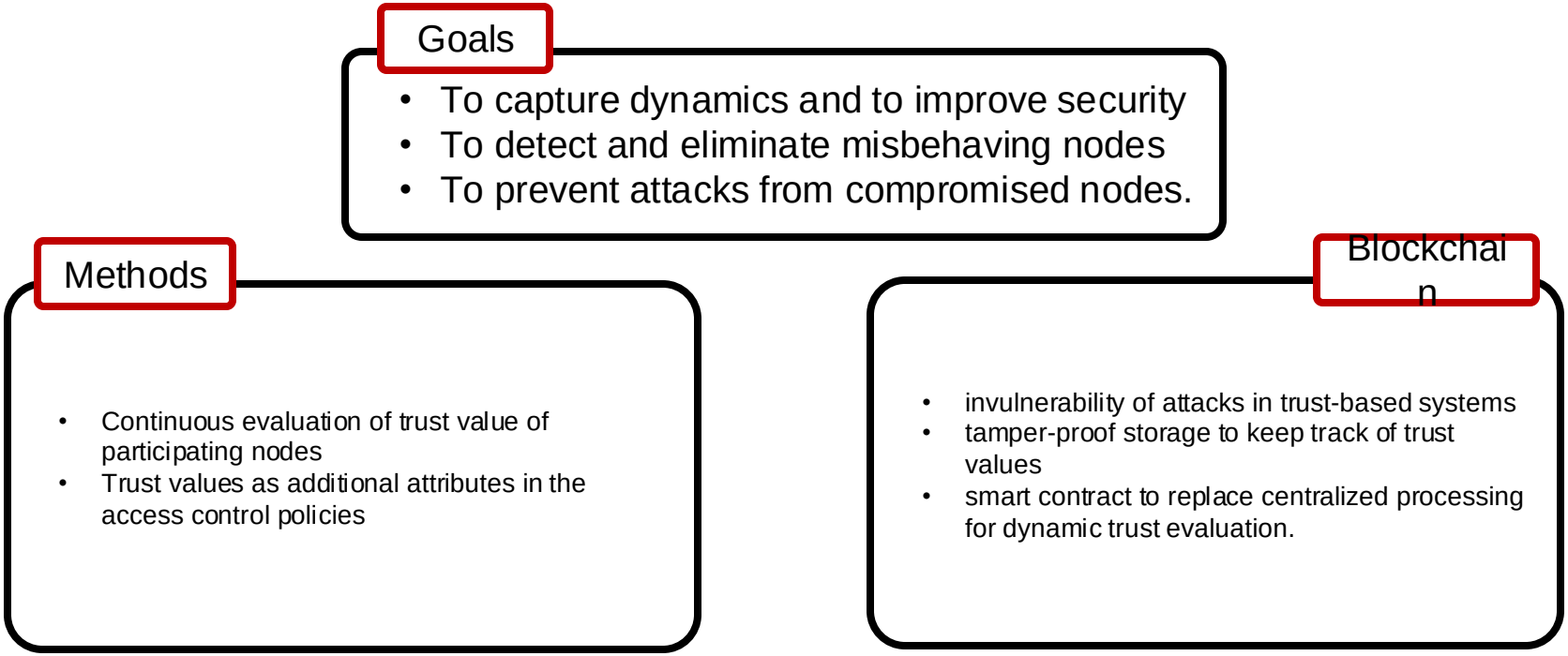
Authorization (Access Control)

- Protect resources from unwanted access.
- Managed by centralized authority.
- Current Schemes: Role-Based, Attribute-Based, Access Control List, etc.

Blockchain for Access Control (AC) in IoT



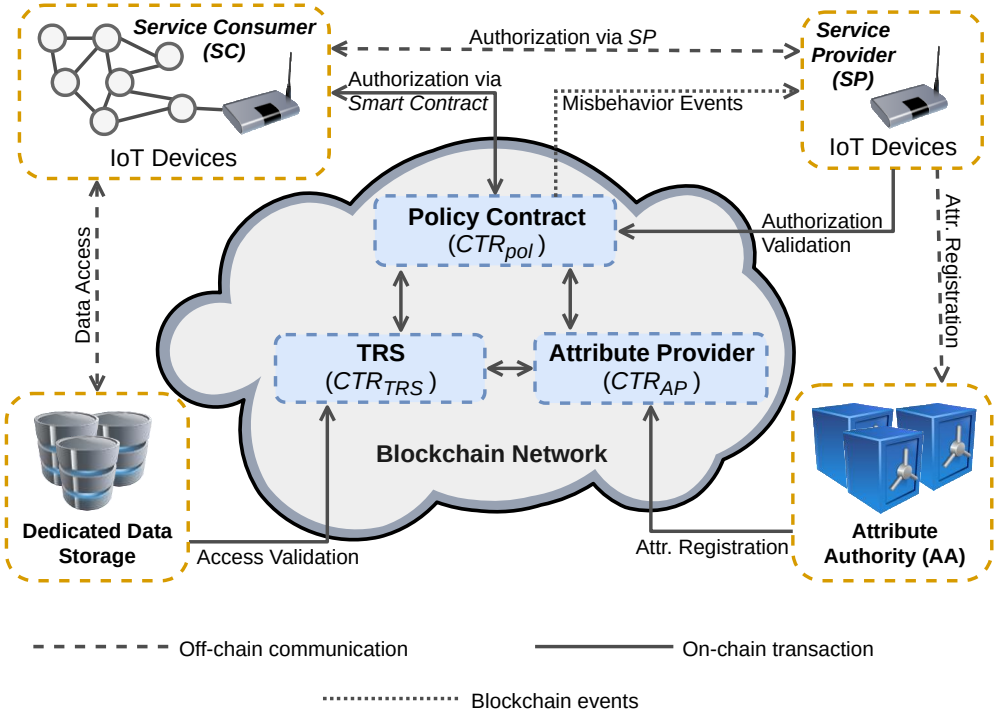
Trust Management in Access Control



System Model – Architectural Components

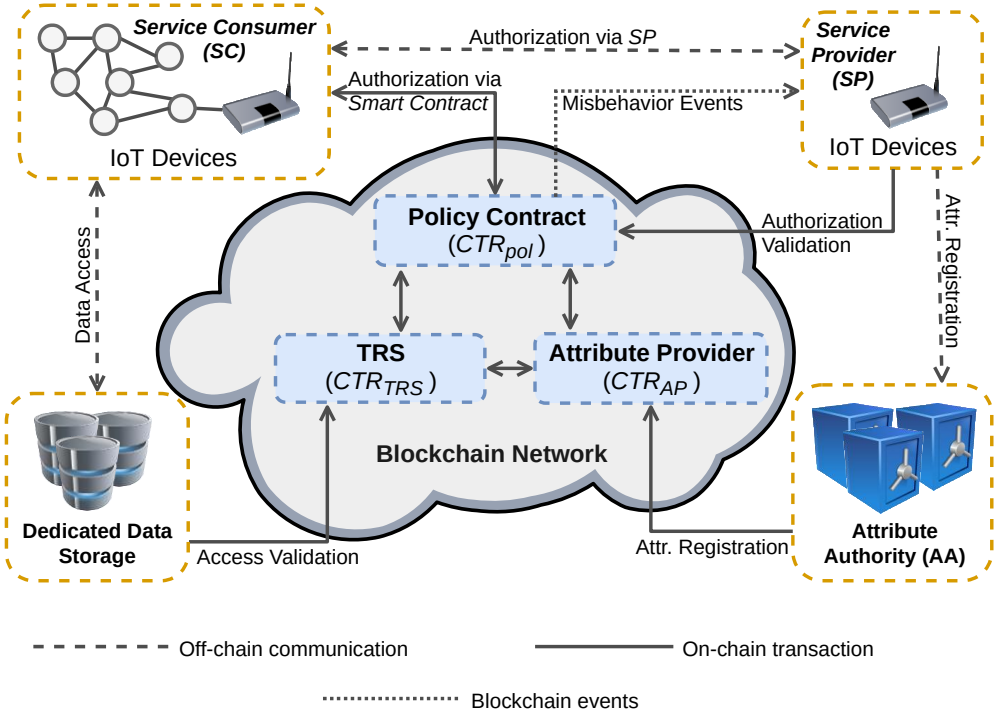
- **Service Consumers (SC)**
  - Request resources
- **Service Providers (SP)**
  - Provide resources
- **Attribute Authority (AA)**
  - Issues legitimate attributes
- **Dedicated Data Storage**
  - Stores data for long timespan (off-chain)
- **Private Blockchain Network**
  - AC logic and policies storage

Public Key as Identifier



System Model – Smart Contracts

- **Policy Contract**
  - Manages access policies
  - Validates access request
- **Trust and Reputation System**
  - Computes reputation score
  - Stores reputation score
- **Attribute Provider**
  - Validates requester's attributes



Trust and Reputation System

Trust

- ***Subjective belief*** that an entity will act honestly.
- Computed and stored on each *SP*
- The trust of a node A may vary across *SP*s.

$$I_n = \sum_{i=1}^{n} \gamma^{(n-i)}.\delta_i$$

Ageing function

$$\delta_i = \begin{cases} \delta_{pos} & \text{If positive interaction} \\ \delta_{neg} & \text{If negative interaction} \end{cases}$$

$$T_{i,j}(I_n) = a.e^{-b.e^{-c.I_n}}$$

Gompertz growth function

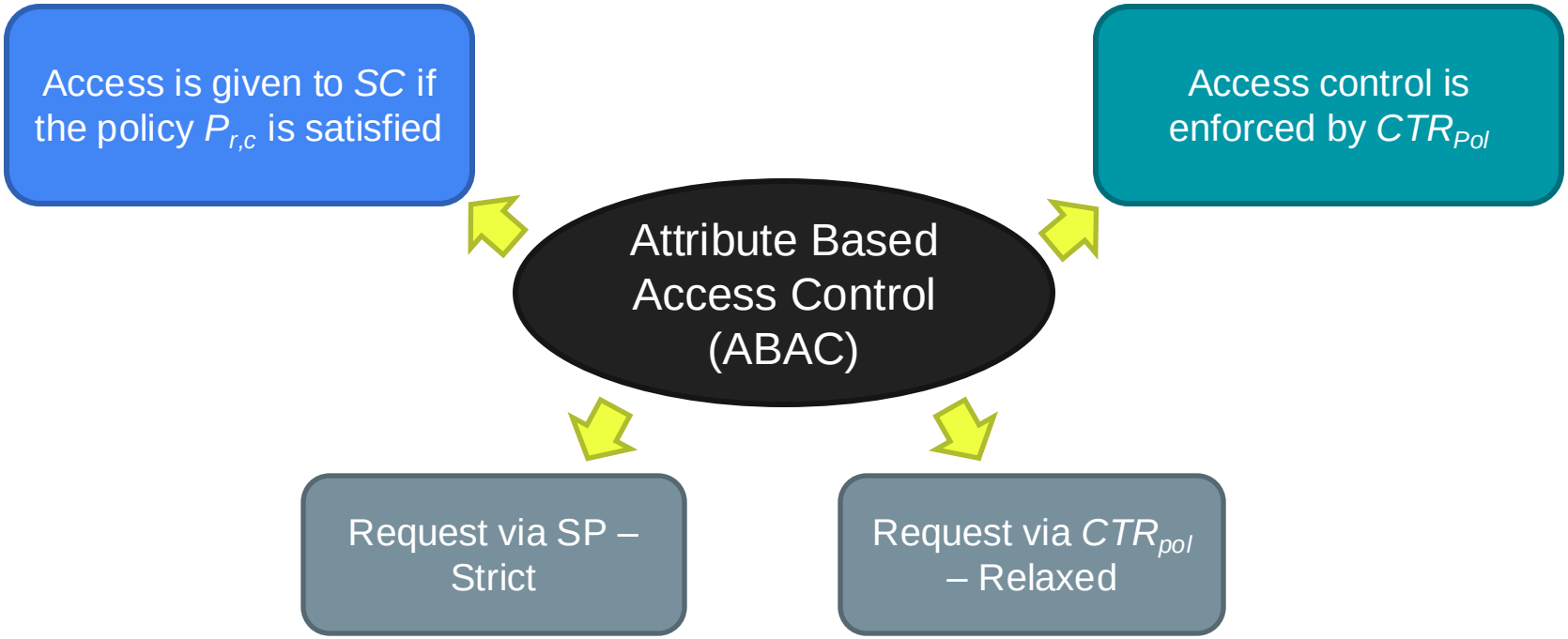
Reputation

- ***Global perception*** of an entity's behavior.
- Collaboratively recorded in the blockchain
- Computed by CTR_{TRS} and stored on the blockchain

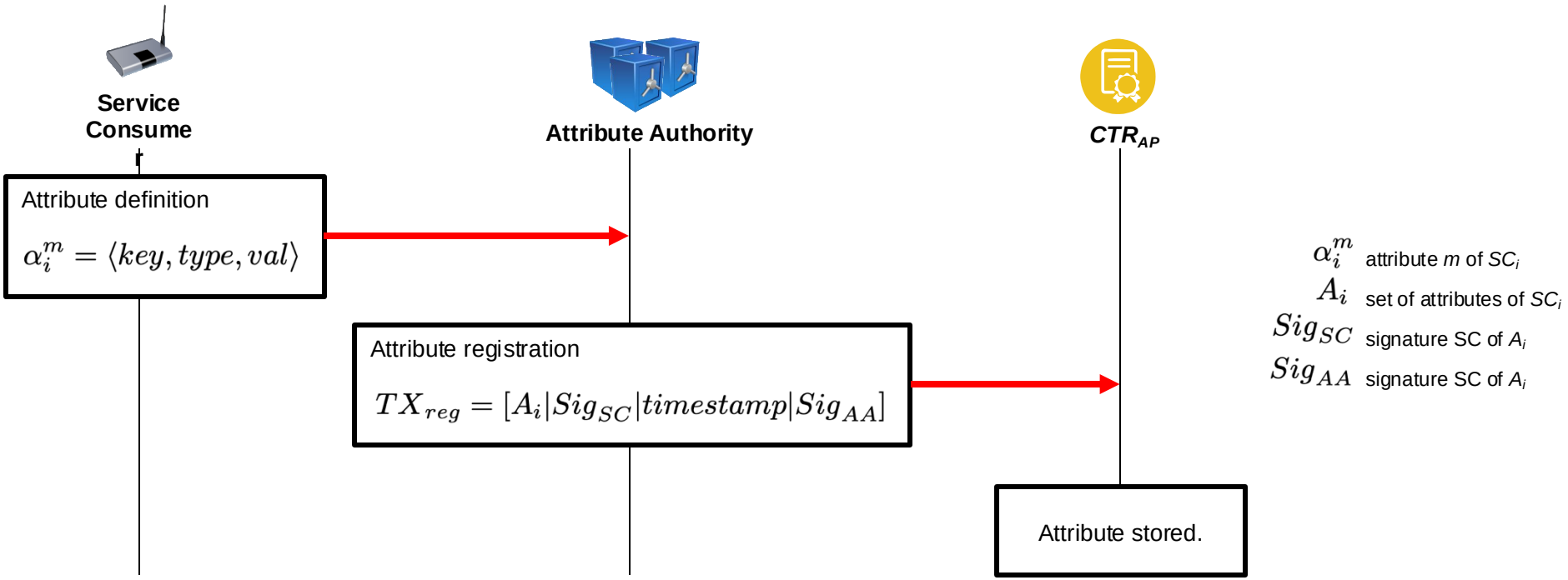
$$Rep_{i,n} = \left(\sum_{t=1}^{n} \beta_t \lambda^{(n-t)} \right) ln(N_{peers})$$

$$\beta_t = \begin{cases} \beta_{pos} & \text{If positive interaction} \\ \beta_{neg} & \text{If negative interaction} \end{cases}$$

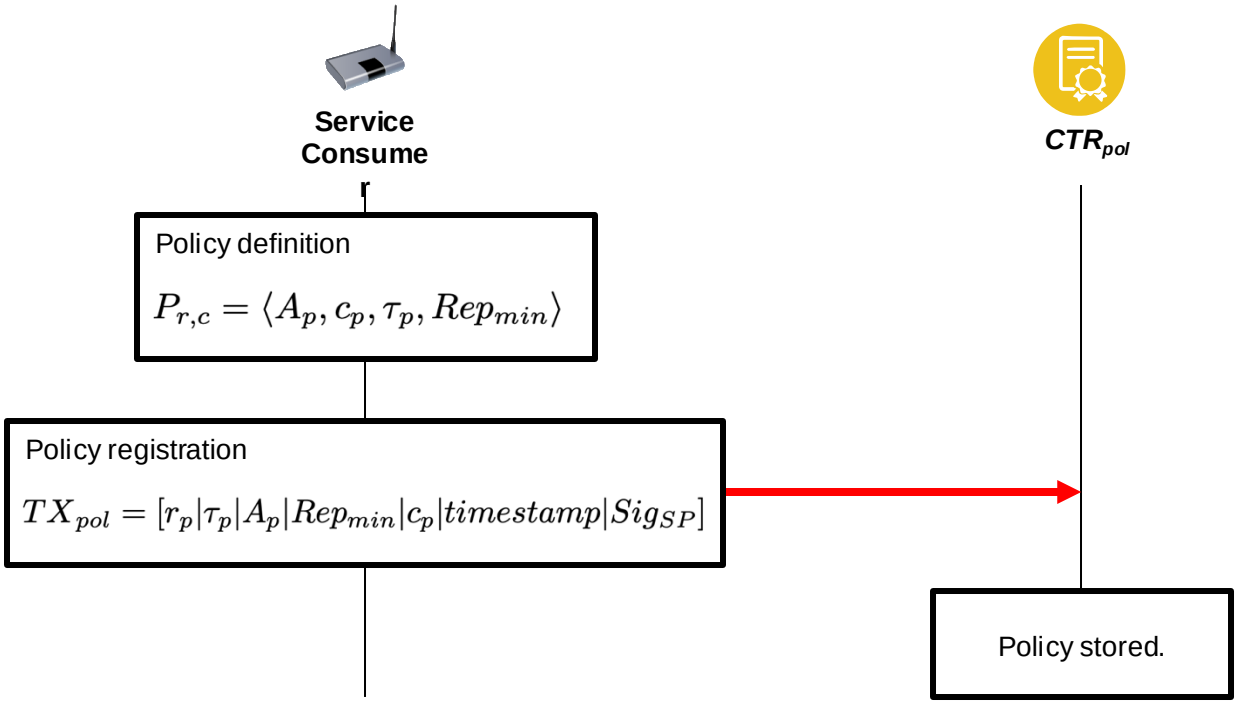
Access Control Scheme



Device Attributes

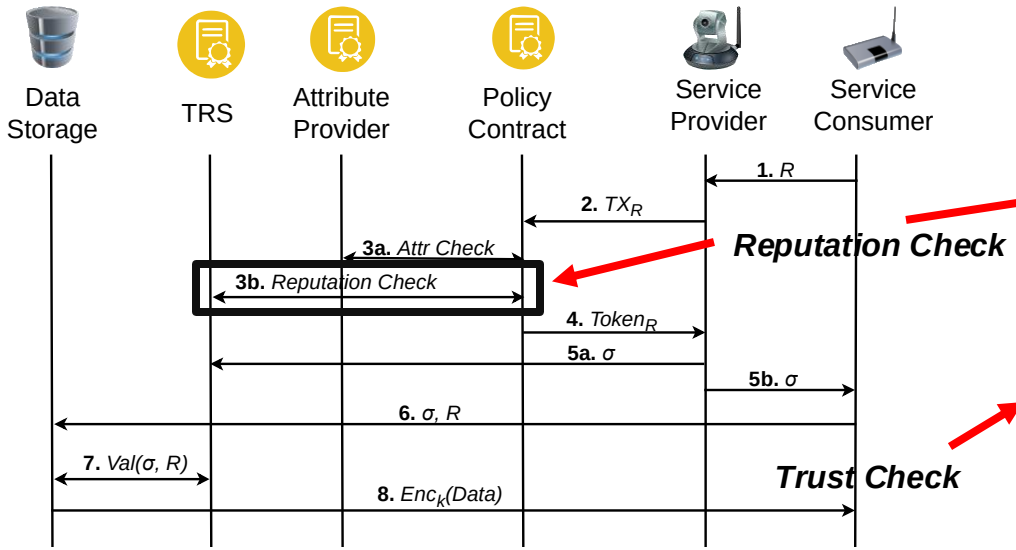


Access Policies



$P_{r,c}$	access policy of resource *r* in context *c*
A_p	set of required attributes
c_p	context
τ_p	set of allowed actions
Rep_{min}	minimum reputation score
r_p	resource identifier
Sig_{SP}	signature of SP

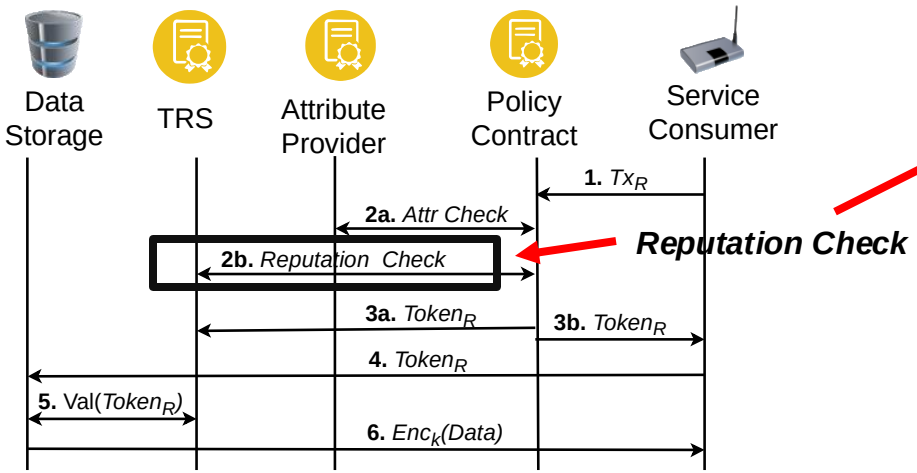
Authorization via SP – Strict



SC authorizes via *SP*

1. $R = \langle r, \tau, S \rangle, Sig^R_{SC}$
2. $TX_R = [r|\tau|S|Sig^R_{SC}|Sig_{SP}]$
3. Attribute and Reputation Check
4. $Token_R = \langle Rep_i, Exp_R, l, t \rangle$
5. Finalization by SP $Decision_{i,k} = g[T_{i,j}, Rep_i]$
   $\sigma = Sig_{SK_{SP}}(Token_R)$
6. $\langle \sigma, R \rangle$
7. Validation
8. Return encrypted data

Authorization via CTR_{pol} – relaxed

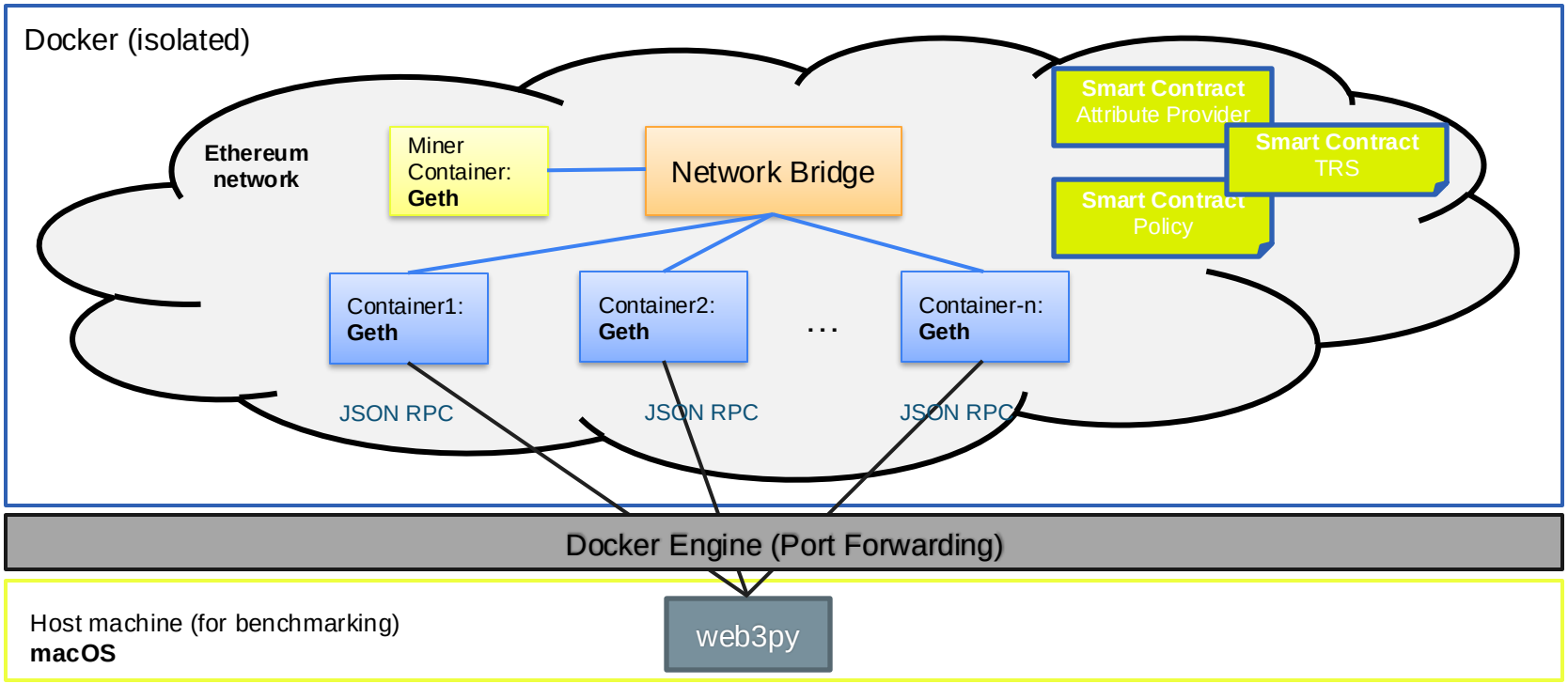


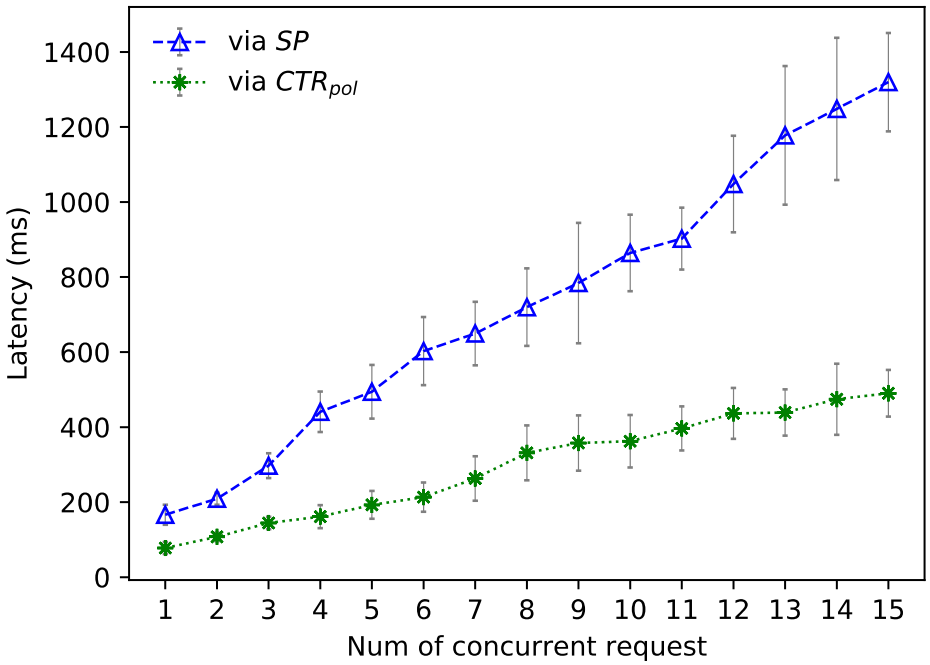
Reputation Check

SC authorizes via *Smart Contract*

1. Without Sig_{SP}
2. Attribute and Reputation Check
3. $Token_R = \langle Rep_i, Exp_R, l, t \rangle$
4. Access request
5. Validation
6. Return encrypted data

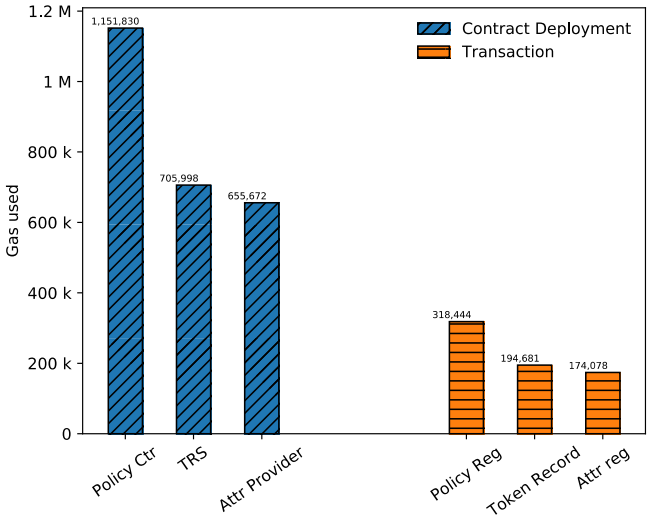
Proof-of-concept Implementation





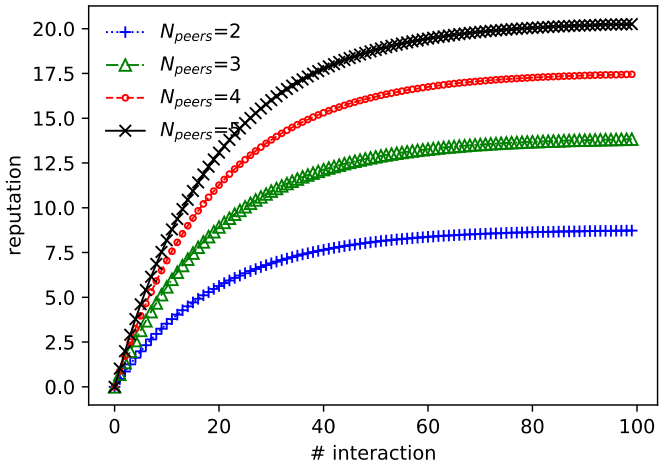
- Simulated in 30 times measurements
- $Latency_{SP} > Latency_{Smart\ Contract}$
- Linear trend in both access type
- Access via SP may introduce bottle neck

- **Policy Contract:**
  - Stores access policy
- **Trust and Reputation System**
  - Record misbehavior and calculate reputation
- **Attribute Provider:**
  - Stores legitimate attributes.



Methods		Type	Gas Used			Elapsed Time (ms)		
Method	Contract		Min	Max	Average	Min	Max	Average
-	CTR_{AP}	Ctr. depl.	-	-	655 608.00± 0.00	1332.3	18 574.65	5724.71± 4.08K
-	CTR_{pol}	Ctr. depl.	-	-	1 654 067.00± 0.00	1331.91	12 074.71	5078.07± 2.83K
-	CTR_{TRS}	Ctr. depl.	-	-	1 036 234.00± 0.00	1158.60	14 877.57	5367.94± 3.12K
regAttr	CTR_{AP}	Func. call	159 014	174 078	159 575.86± 2.69K	1031.16	9150.20	4784.21± 1.89K
regPolicy	CTR_{pol}	Func. call	303 422	318 422	303 922.00± 2.69K	605.43	25 747.86	5795.94± 5.38K
recMsbehavior	CTR_{TRS}	Func. call	100 055	195 334	103 230.97± 1.71K	1580.69	12 177.24	5092.43± 2.65K

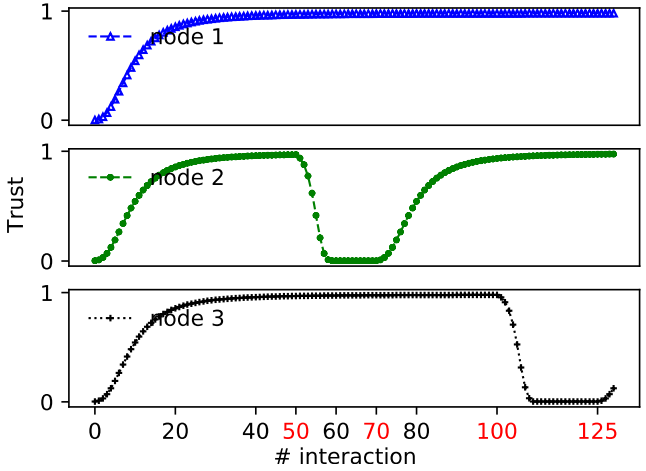
Reputation



$$Rep_{i,n} = \left(\sum_{t=1}^{n} \beta_t \lambda^{(n-t)}\right) ln(N_{peers})$$

- Beta: 10
- Lambda: 0.95

Trust



$$I_n = \sum_{i=1}^{n} \gamma^{(n-i)}.\delta_i$$

Ageing function

$$T_{i,j}(I_n) = a.e^{-b.e^{-c.I_n}}$$

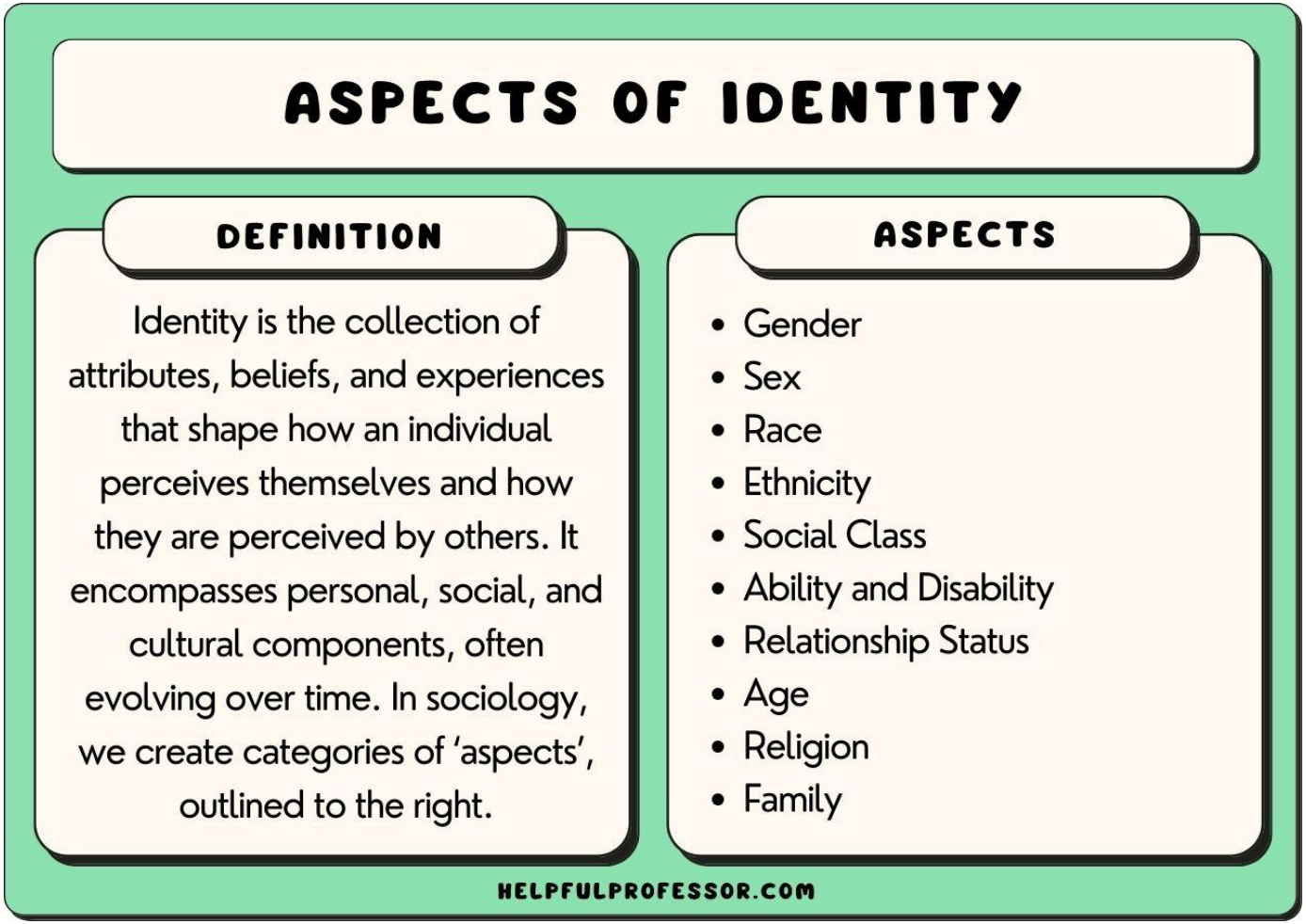
Gompertz growth function

- Gamma: 0.95
- a: 1 (asymptote)
- b: -6 (x-axis displacement)
- c: -0.1 (growth rate)

Summary

- Authentication and authorization are necessary in computer systems, even for IoT.
- IoT needs special requirement for authentication and authorization.
- Centralization has its own drawbacks, especially single point of failure.
- Blockchain has the potential of improving authorization scheme for IoT.
- Trust management has the potential to achieve a dynamic and flexible access control.

Self-Sovereign Identity



A ***credential*** is a ***piece of any document*** that details a *qualification*, *competence*, or *authority* issued to an ***individual*** by a third party with a relevant or de facto authority or assumed competence to do so.

- Wikipedia

Problems with digital credential sharing

- Single point failure
- Hard to achieve trust between sharing parties
  - Cannot be easily verified online
  - Disclose more than necessary (oversharing)

CNBC INDONESIA

HOME MARKET INVESTMENT NEWS ENTREPRENEUR SYARIAH TECH LIFESTYLE IN

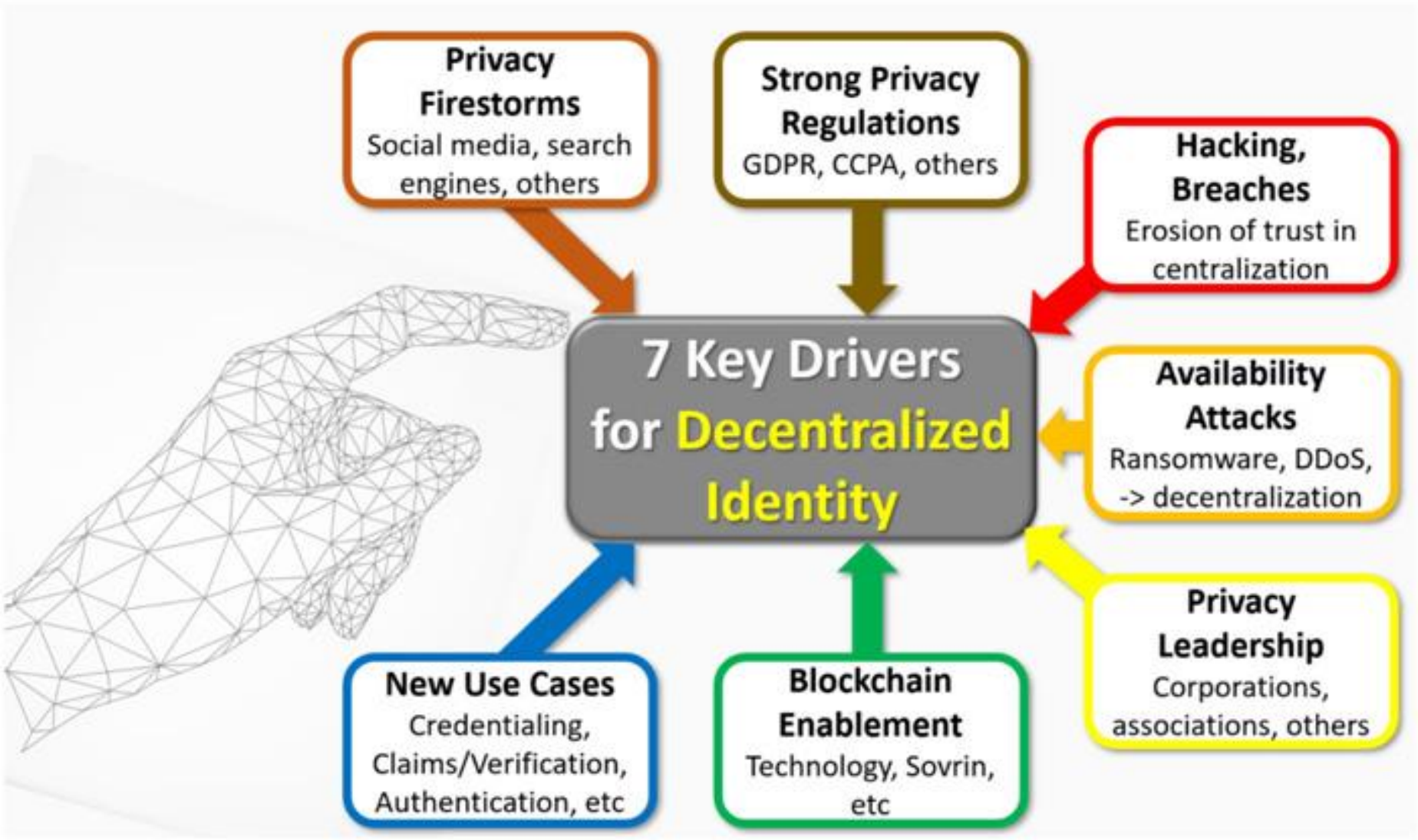
FOTO VIDEO INFOGRAFIS

CNBC Indonesia > Tech > Berita Tech

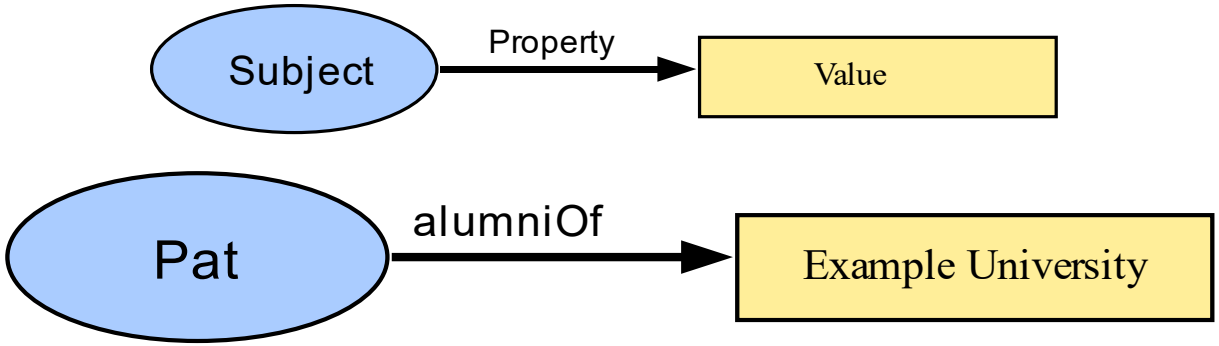
Heboh! Data KTP Hingga Nomor HP 279 Juta Warga RI Bocor?

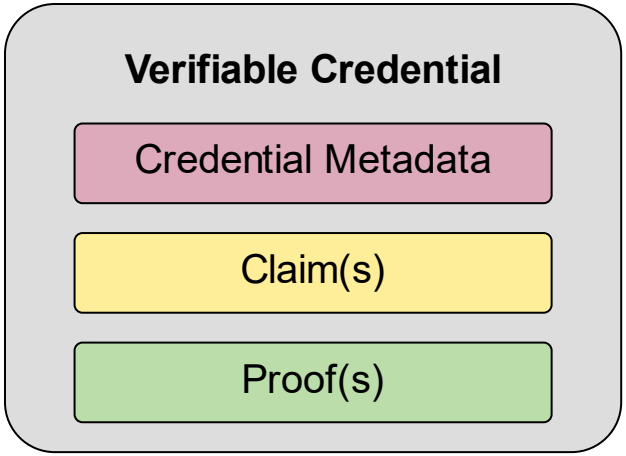
TECH - roy, CNBC Indonesia | 20 May 2021 16:17

SHARE |

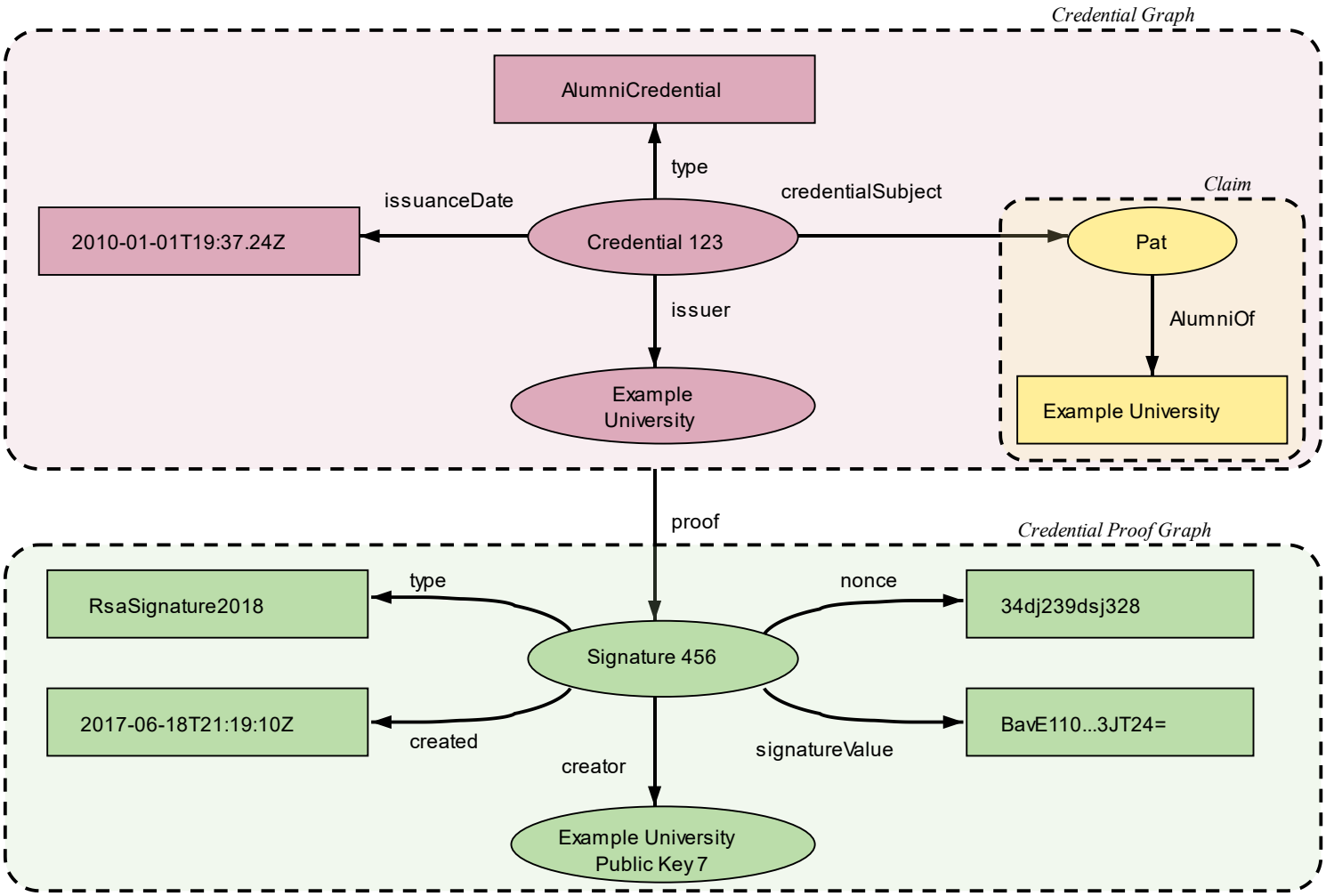

Privacy Firestorms
Social media, search engines, others
Strong Privacy Regulations
GDPR, CCPA, others
Hacking, Breaches
Erosion of trust in centralization
7 Key Drivers for Decentralized Identity
Availability Attacks
Ransomware, DDoS, -> decentralization
Privacy Leadership
Corporations, associations, others
New Use Cases
Credentialing, Claims/Verification, Authentication, etc
Blockchain Enablement
Technology, Sovrin, etc

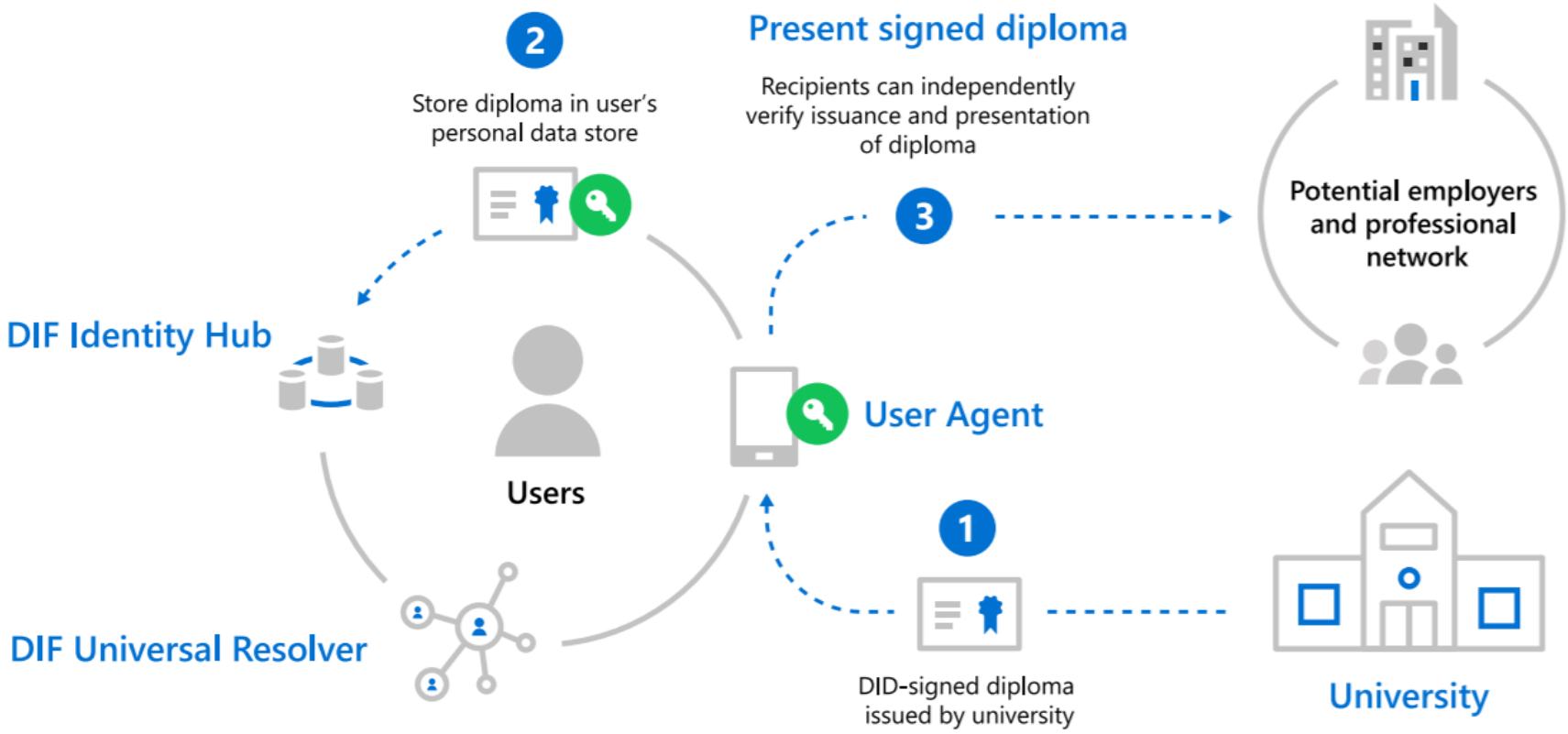
Data Model – Verifiable Credentials





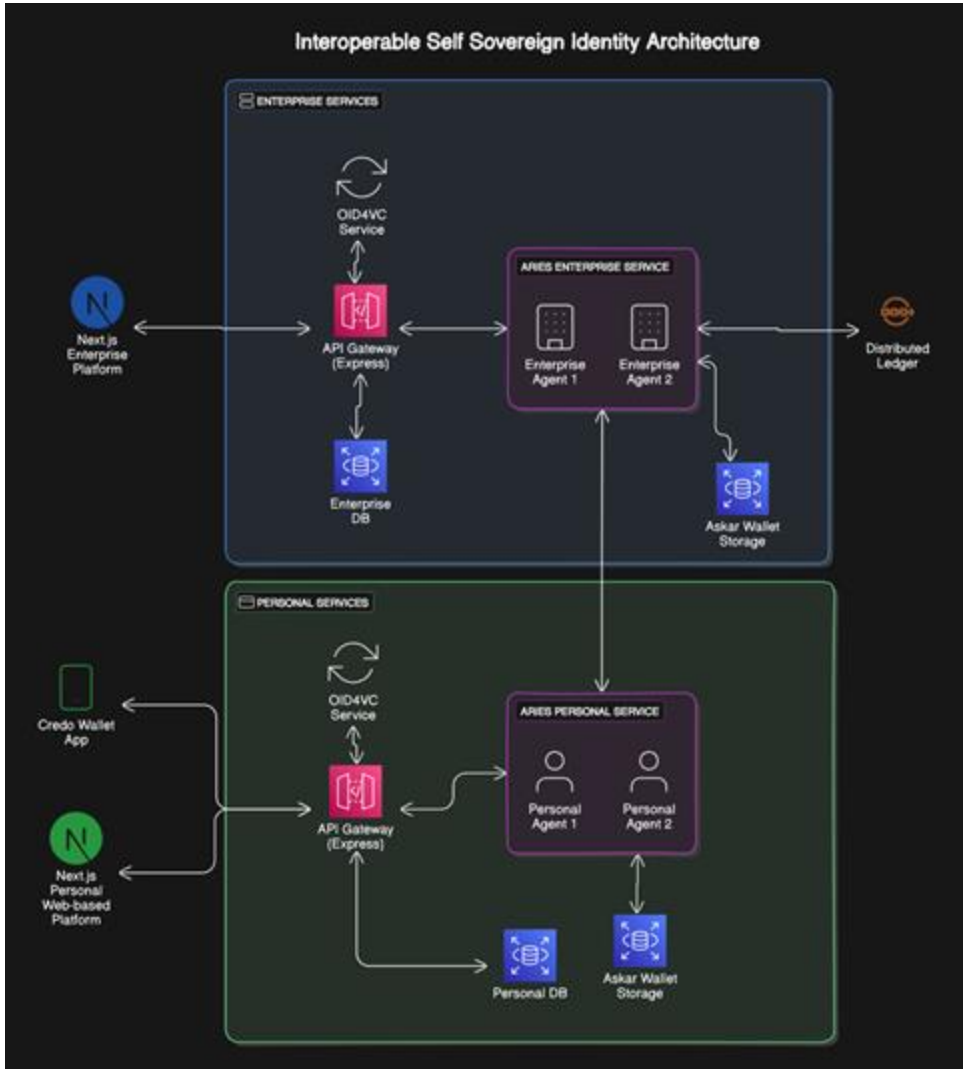
Data Model – Verifiable Credentials (2)

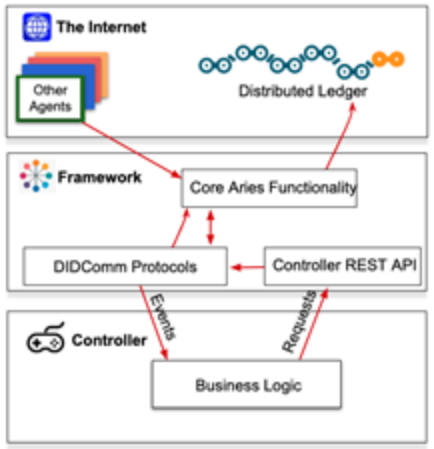




Microsoft Decentralized ID whitepaper

Interoperable Self Sovereign Identity Architecture





Thank you


Scheme
did:example:123456789abcdefghi
DID Method
DID Method-Specific Identifier

The standard elements of a DID doc

1. **DID** (for self-description)
2. **Set of public keys** (for verification)
3. **Set of auth methods** (for authentication)
4. **Set of service endpoints** (for interaction)
5. **Timestamp** (for audit history)
6. **Signature** (for integrity)