Blockchain solutions for IoT security and privacy

Djamel Eddine Kouicem

Heudiasyc, UMR CNRS, Université de Technologie de Compiègne

dkouicem@hds.utc.fr

June 4th, 2020

Academic and professional Curriculum

R&D Internship at CDTA, Algiers

2015

R&D Internship at Orange Labs., Châtillon, France

March 2016

ATER at UTC

Nov. 2019

Present

- November 2019: **PhD** (BAC + 8) in Computer science, Université de Technologie de Compiègne (UTC)

  Thesis: Security of the Internet of Things for systems of systems

  Advisor: Pr. Abdelmadjid Bouabdallah

- August 2016: **Master Degree** (BAC + 5) in Computer science and Networking, University of Paris 6 (UPMC), Option: **Networking and Cloud Infrastructure**

- June 2015: **Engineer** (BAC + 5) in Computer science, Ecole nationale supérieure d'Informatique, Algiers, Algeria

Outline

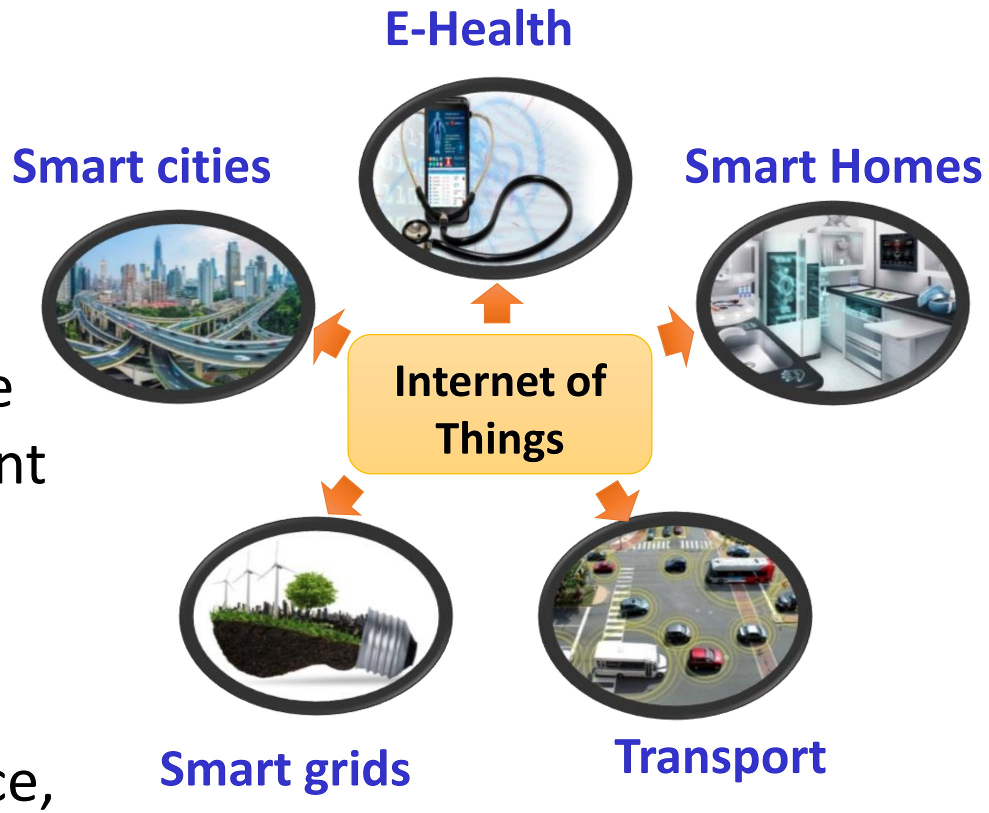
1. Context
2. Backgrounds (IoT security, blockchain)
3. Blockchain-based security solutions for IoT
4. A blockchain-based anonymous data sharing protocol for VANETs
5. Conclusion & Perspectives

- **Internet of Things (IoT)** is a new emerging technology that consists to connect physical world to Internet

- IoT is an enabling technology for Cyber-Physical Systems **(Systems of Systems)**

- **A System of Systems (SoS)** is an integration of a finite number of constituent systems which are independent and work together to achieve a high common goal

- **IoT based SoS characteristics**: Operational and managerial independence, Evolutionary independence, Geographic distribution, Emergent behavior



IoT Applications

1. Context (cont.)

IoT security/privacy : an important challenge

- Security is on the top of important issues in IoT
- In recent years, **52%** of connected objects had no security countermeasures
- IoT operates in open environments, exposed to various malicious attacks
- IoT security is deeply linked to people's daily lives
- Traditional security solutions are inapplicable in the context of IoT due to **limitation of resources**, **scalability issues**, **heterogeneity**, etc.

2.1 Background on Security Services

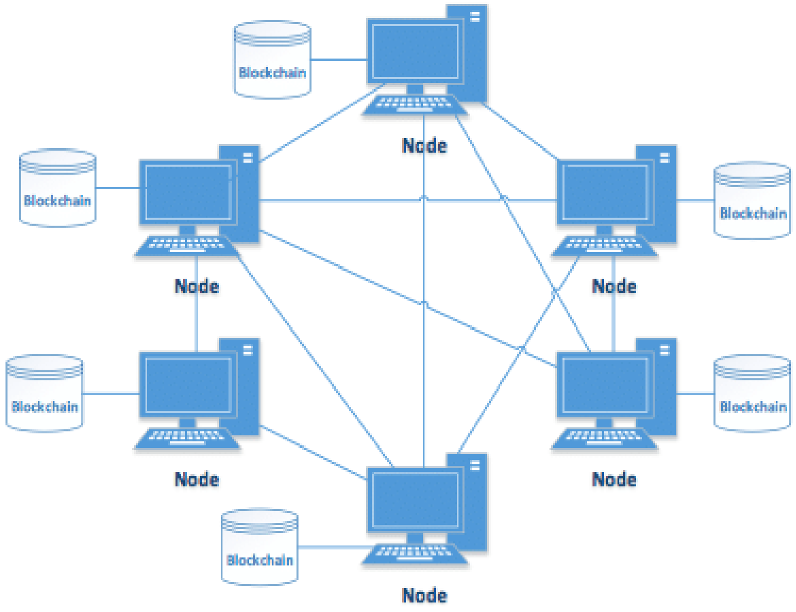
- Several security services need to be ensured in IoT:
  - Authentication of IoT devices
  - Data confidentiality
  - Data Integrity
  - Availability
  - Trust management
  - Data privacy

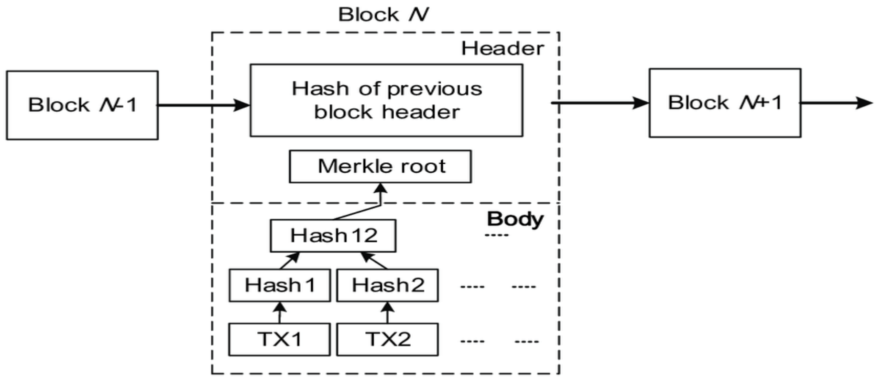
Cryptographic tools

+

Blockchain technology

- The blockchain is a decentralized database which is duplicated and shared by nodes communicating via Peer to Peer infrastructure
- No central entity that controls the whole blockchain
- The blocks are connected to each others. Each block contains the hash of its previous block
- Each block is validated by blockchain validators based on a consensus protocol (PoW, PoS, PBFT, etc.)
- Blockchain allows: **immutability, traceabality, no single point of trust, transparency**





My research activities

My contributions

- Authentication in the IoT/Fog [Trustcom 18]
- Access control in the IoT [IEEE ISPA 17]
- Trust management in the IoT [IEEE SoSE 18, IEEE TDSC]
- Survey in IoT security [COMNET, 2018]
- Data privacy protection in VANETs [IEEE ISCC 2020]

International journals (**x2**)	**International conferences** (**x6**)
• Computer Networks (Elsevier, IF: **3.030)** • IEEE Trans. on Dependable and Secure Computing (IF: **6.404**) **Submitted journal papers**: IEEE Trans. on Dependable and Secure Computing (IF: **6.404)**	IEEE Globecom 2017, IEEE/IFIP IM 2017, IEEE ISPA 2017, IEEE SoSE 2018, IEEE Truscom 2018, IEEE ISCC 2020 **Submitted papers**: IEEE Globecom 2020
Total : 2 et 1 submitted	**Total : 6 et 1 submitted**

My research activities

Blockchain-based security solutions for the IoT/fog applications

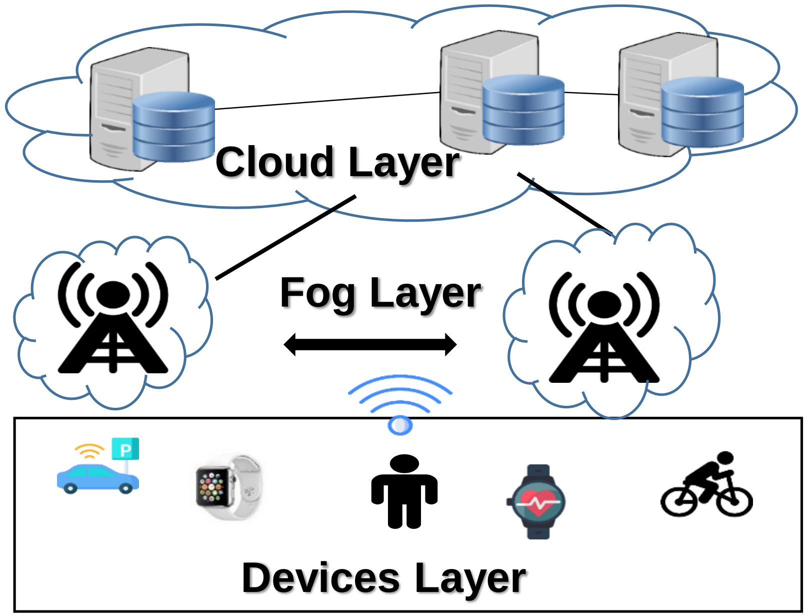
- ❑ Extension of cloud services at the edge of the IoT (fog computing)
- ❑ Many security challenges related to IoT/fog/Cloud : trust management, authentication, etc

Mutual authentication at IoT/fog/cloud

- ➢ Blockchain as a secure database to store fog nodes' public keys
- ➢ Threshold cryptography to authenticate the IoT devices

Trust management in IoT

- ➢ Decentralized trust management protocol
- ➢ Support the mobility of IoT devices

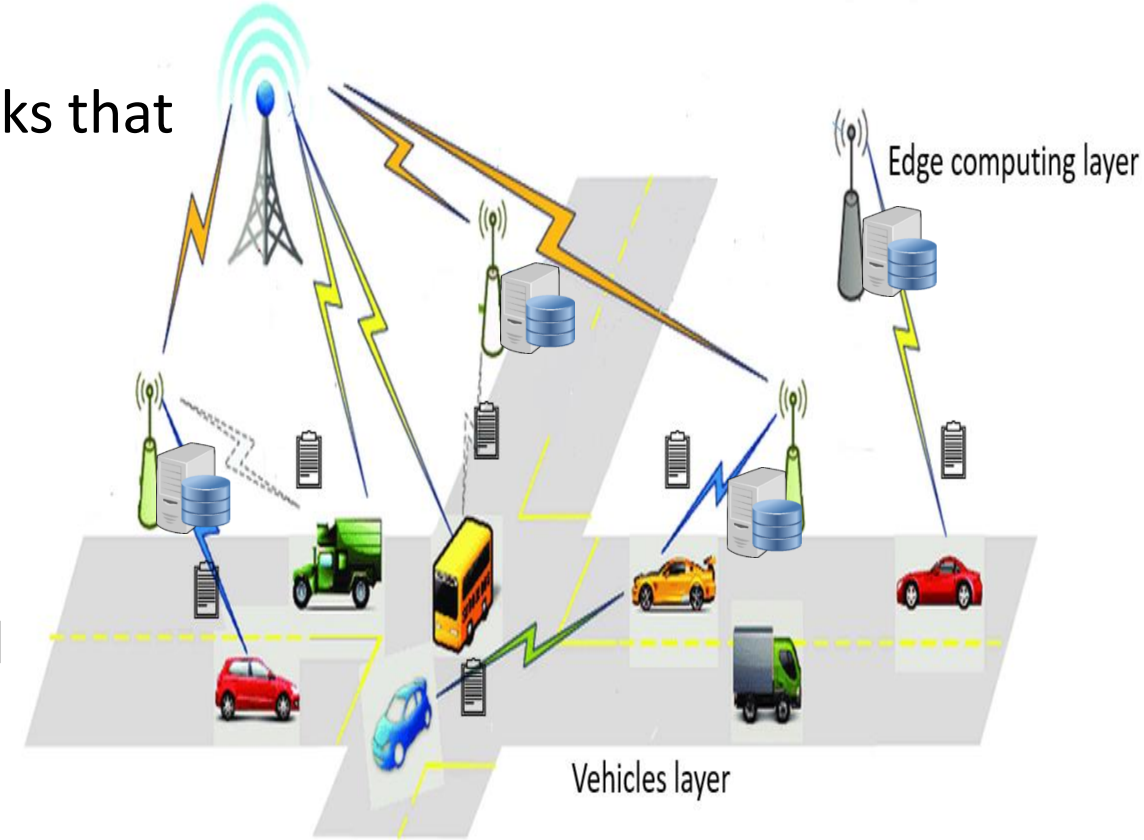


A blockchain-based anonymous data sharing scheme for VANETs [4]

[4] **Kouicem, D. E.,** Bouabdallah, A., Hicham, L. *An Efficient and Anonymous Blockchain-Based Data Sharing Scheme for Vehicular Networks*. In the 25th IEEE Symposium on Computers and Communications.

Problem: How to develop an **anonymous** data sharing protocol in VANETs ?

- ❑ Vehicles generate complex and sensitive traffic data
- ❑ VANETs are subjected to several malicious attacks that threaten the privacy of conductors

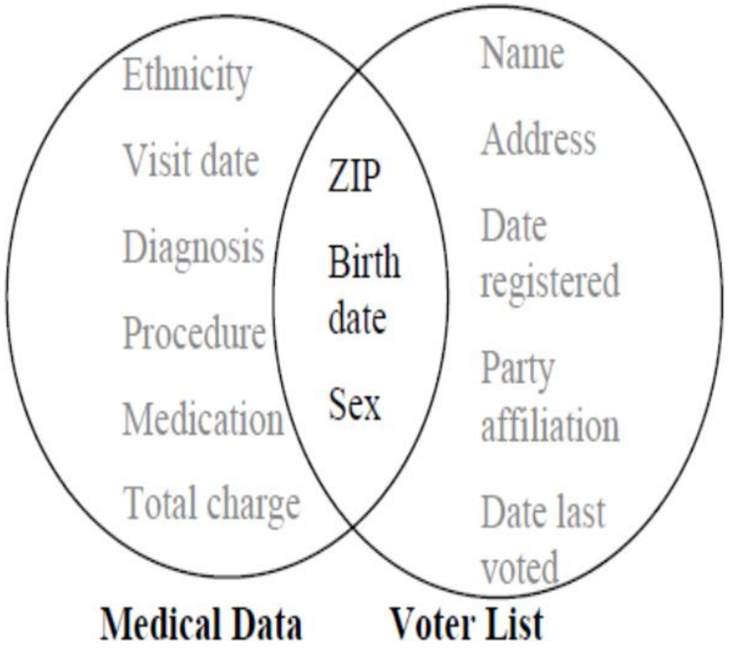


Our **Data sharing** protocol:

- ➢ supports the **mobility** of vehicles,
- ➢ **protects the privacy** of the conductors, and
- ➢ does not need a **pre-trusted entity** in the whole system.

3.2 Data privacy protection

- 87% of americans can be identified only with the triplet (birthday, Sex, ZIP)
- Data privacy protection requieres anonymization techniques (k-anonymity, l-diversity, differential privacy)
- **Definition : Working group G29 (GDPR)**
  - **Individualization**: is it possible to separate a person from
  - **Non correlation**: is it possible to link separate datasets together concerning the same individual ?
  - **Inference**: can we deduce information about an individual ?



Source: [Sweeney, 2002]

K-anonymity and l-diversity models

Original dataset

id	Zipcode	Age	National.	Disease
1	13053	28	Russian	Heart Disease
2	13068	29	American	Heart Disease
3	13068	21	Japanese	Viral Infection
4	13053	23	American	Viral Infection
5	14853	50	Indian	Cancer
6	14853	55	Russian	Heart Disease
7	14850	47	American	Viral Infection
8	14850	49	American	Viral Infection
9	13053	31	American	Cancer
10	13053	37	Indian	Cancer
11	13068	36	Japanese	Cancer
12	13068	35	American	Cancer

4-anonymous data

id	Zipcode	Age	National.	Disease
1	130**	<30	*	Heart Disease
2	130**	<30	*	Heart Disease
3	130**	<30	*	Viral Infection
4	130**	<30	*	Viral Infection
5	1485*	≥40	*	Cancer
6	1485*	≥40	*	Heart Disease
7	1485*	≥40	*	Viral Infection
8	1485*	≥40	*	Viral Infection
9	130**	3*	*	Cancer
10	130**	3*	*	Cancer
11	130**	3*	*	Cancer
12	130**	3*	*	Cancer

3.2 State of the art of data privacy techniques

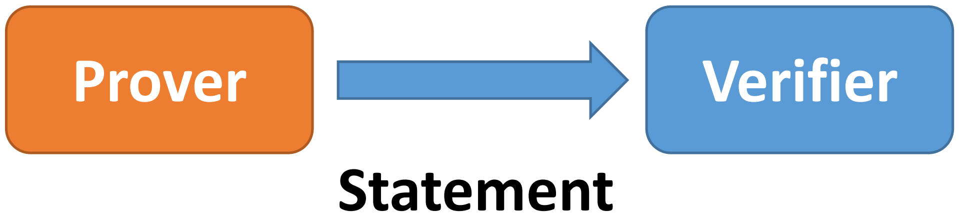
Data Privacy

- K-anonymity / l-diversity
  - K-anonymity for data analytics. [M Satyanarayanan et al.,2015]
  - K-anonymity-based location privacy-preserving [wang et al., 2013]
- Cryptographic techniques
  - Zero Knowledge proofs [Chatzigiannaki s et al., 2015]
  - Ring Signatures [J Liu et al., 2019]
- Data tagging
  - Data tagging for IoT [Evans et al., 2012]
- Data obfuscation
  - Data disclosure for IoT [Tonyali et al., 2017]

3.2 Zero-Knowledge Proof (ZKP)

Definition:

Cryptographic tool that enables a **Prover** to convince a **Verifier** of the validity of a **statement.** It verifies the following requirements:

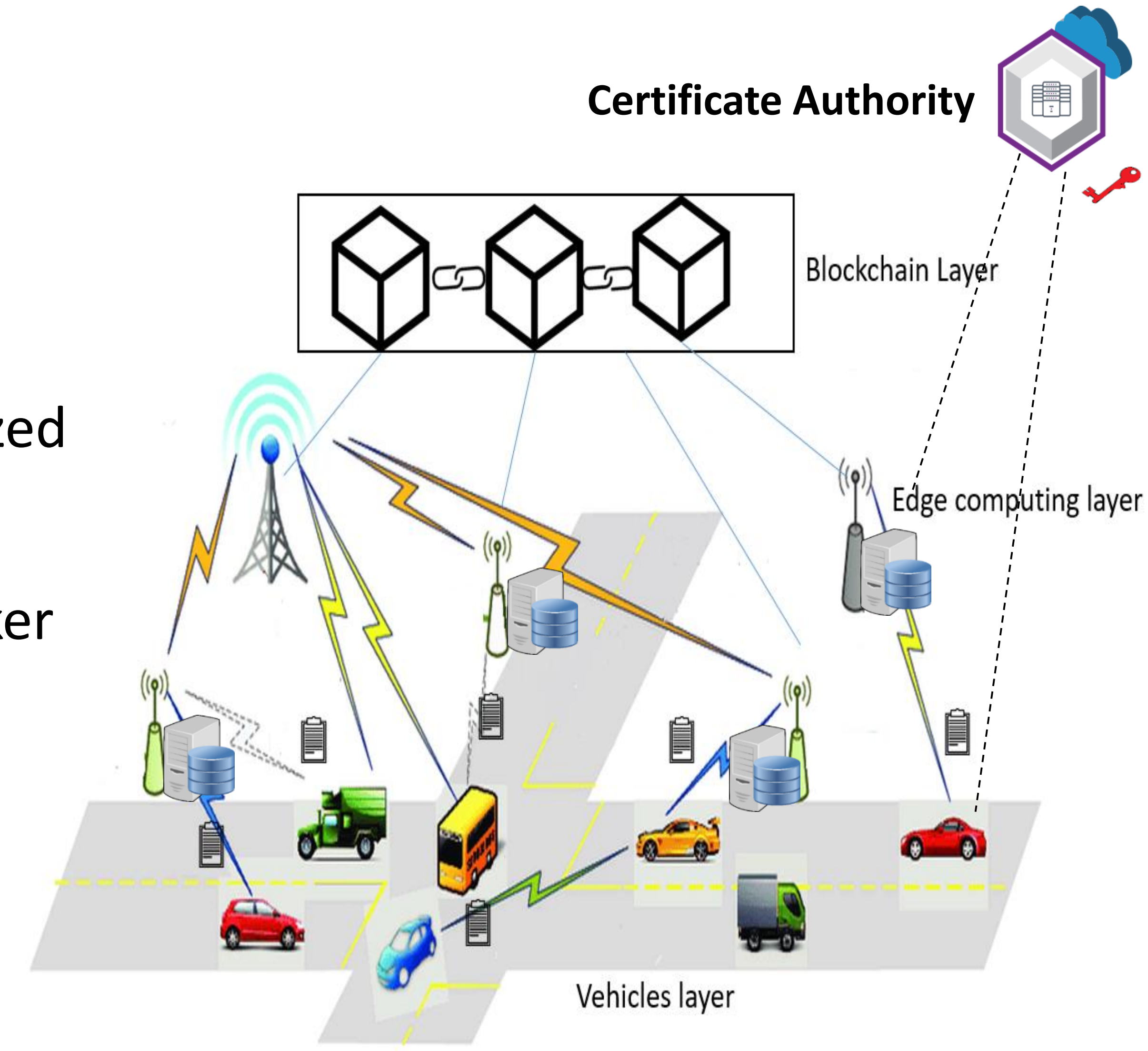


- **Completeness:** If the statement is true, the **Prover** will be able to convince any honest **Verifier**
- **Soundness:** If the statement is false, a **cheating Prover** cannot convince any honest **Verifier** that it is true
- **Zero-Knowledge:** The **Prover** does not reveal anything excepts the validity of the statement

Non-Interactive ZKP: there is no multiple exchanges between the **Prover** and the **verifier**

3.2 Our solution

- **The consortium blockchain** is maintained by powerful edge nodes
- The blockchain is used to store the **indexes** to raw data and proof of **its authenticity**
- The storage of data is done using a decentralized **publish-subscribe** model (ex. MQTT):
  - Each Edge node is served as a MQTT brocker
  - Vehicles are subscribers/publishers in our model
- The authentication of data is based on **ZKP**



3.2 System initialisation

1. Generation of public parameters by Certicicate Authority (CA)

$$params = \{g_1, g_2, \hat{e}, \quad aud_{pk}, \quad H\}$$

2. Generation of Edge RSU keys

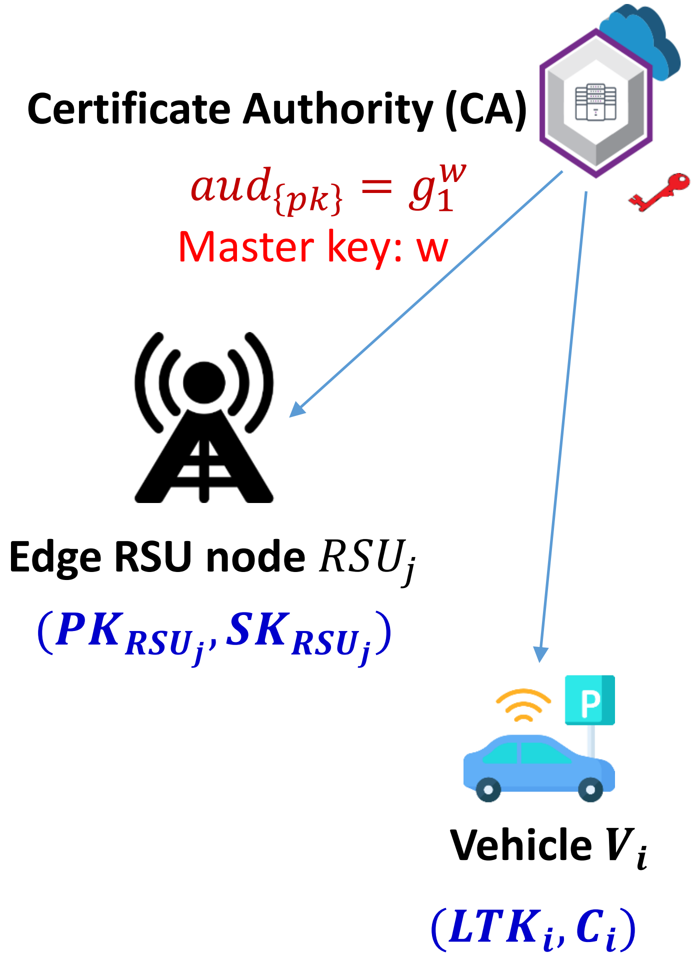
- CA generates a public and private keys (PK_{RSU_i}, SK_{RSU_i})

3. Generation of vehicles' keys

- CA generates a long term public and private pair keys

$$LTK_i = \{PK_i = (g_1^{x_1}, g_1^{x_2}), SK_i = (x_1, x_2)\}$$

- CA generate a certificate $C_i = \left(F_i = (g_1 g_1^{x_1} g_1^{s})^{\frac{1}{\beta+w}}, w, s\right)$



3.2 Generation of the ZKP

1. Generation of one-time public/private keys

- Vehicle V_i picks a random $r_d \in Z_p$ and generates the one-time keys:

$$OTK_i = \{otpk_i = g_1^{x1} g_1^{H\left(g_1^{x_2 * r_d}\right)}, \; otsk_i = x_1 + H(g_1^{r_d})\}$$

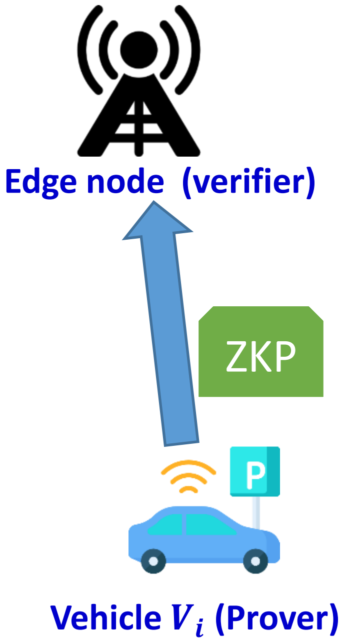
2. Generation of ZKP by the vehicle V_i [Elli et. al, Zerocash 2014]

- Vehicle V_i generates a proof that the OTK_i is computed based on its long term key

$$C_r = (C_{cert} = g_1 . aud_{pk}^{r_{cert}}, \quad B_{cert} = g_1^{r_{cert}})$$

$$\Theta = F_i^{\rho}, R_c = \hat{e}(g_1 C_{cert}^{r_1} g_1^{r_2} \Theta^{-r_3} aud_{pk}^{-r_4}, g_2)$$ $\rho, r_{cert}, r_1, r_2, r_3, r_4$ are randomly generated

- Vehicle V_i generates the challenge: $c = H_1(timestamp||h||C_r||\Theta||R_c)$
- It computes the values : $z_1 = r_1 + c.\rho, \; z_2 = r_2 + c.\rho.s, \; z_3 = r_3 + c.w, \; z_4 = c.r_{cert}.\rho$
- It outputs the Zero-Knowledge Proof : $\mathrm{ZKP} = (c, z_1, z_2, z_3, z_4)$



1. Raw Data uploading

- Vehicle V_i generates a raw data D and sign it using its short term secret key $otsk_i$

  signature : $\sigma = \{D\}_{otsk_i}$

  $$metadata = (timestamp||otpk_i||ZKP||\Theta||description||\sigma||C_r)$$

- Vehicle V_i send the raw data D alongside the $metadata$ to one edge node

2. Verification and storage of raw data By Edge Nodes

- Check the correctness the signature σ using the one-time public key $otpk_i$
- Check the correctness of ZKP proof

  $$R_c' = \hat{e}(g_1 C_{cert}^{z_1} g_1^{z_2} \Theta^{-z_3} aud_{pk}^{-z_4}, g_2).\hat{e}(\Theta, aud_{pk})^{-c}$$

  Check if $c = H(timestamp||otpk_i||C_r||\Theta||R_c')$

- Validate and store the metadata into the blockchain

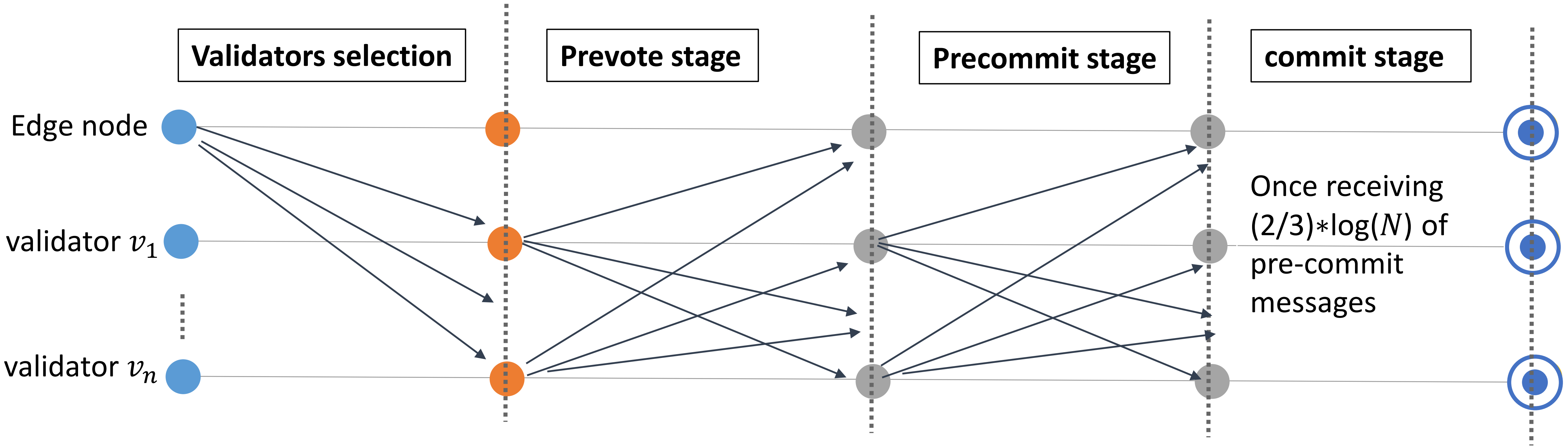
3.4 Our consensus protocol

✿ **Assumption**: there is at least (2/3)*N+1 of nodes that are not faulty and trusted. N is the number of edge servers (validator nodes).

- **Our enhanced PBFT:** the edge node chooses $\boldsymbol{log(N)}$, instead of all the $\boldsymbol{N}$ validators, based on:

$$P_{seletion}(v_i) = \frac{C_i}{\sum_{k=1}^{N} C_k}$$

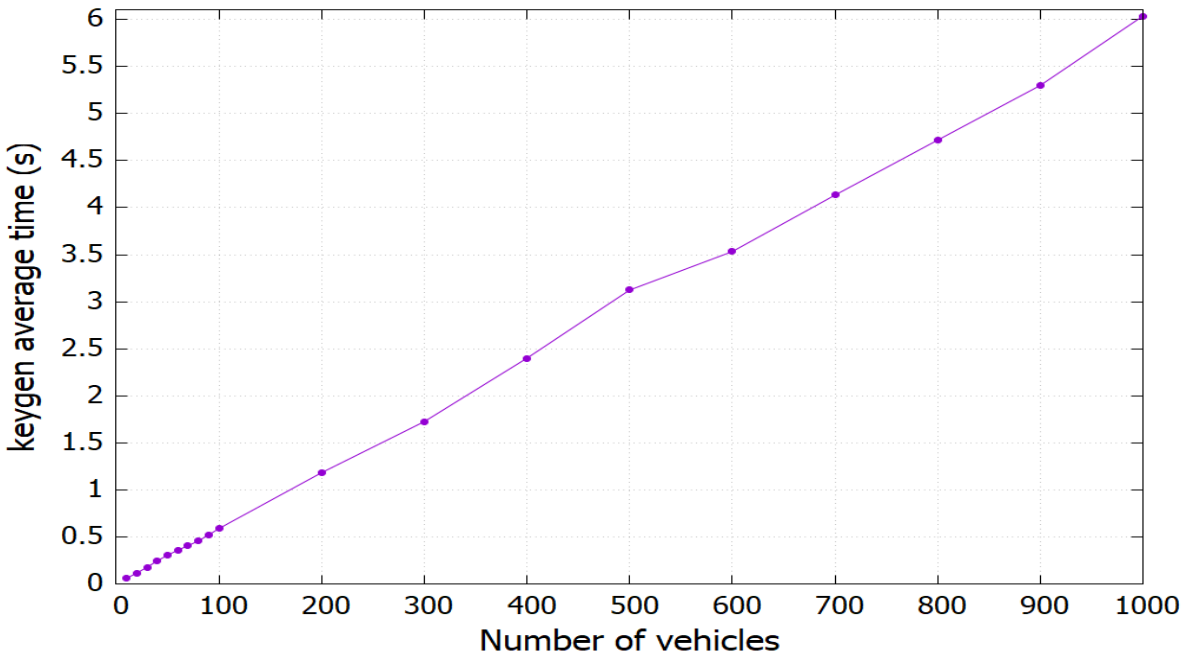
C_i: the storage capacity of the validator v_i

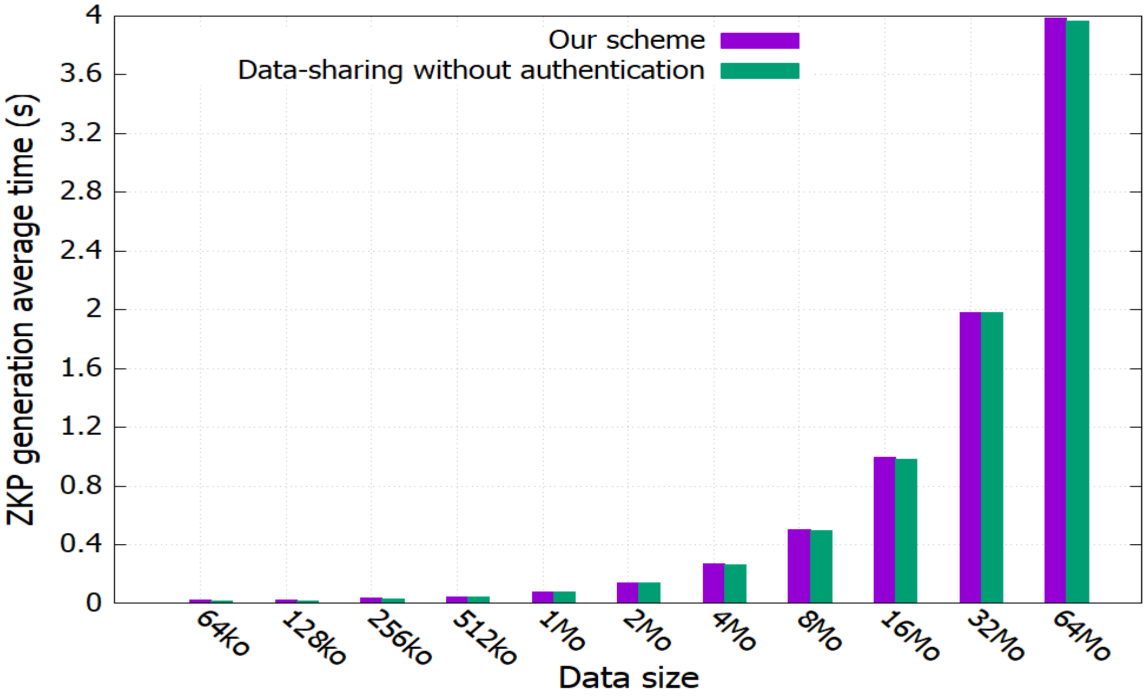


3.5 Performance analysis (1/2)

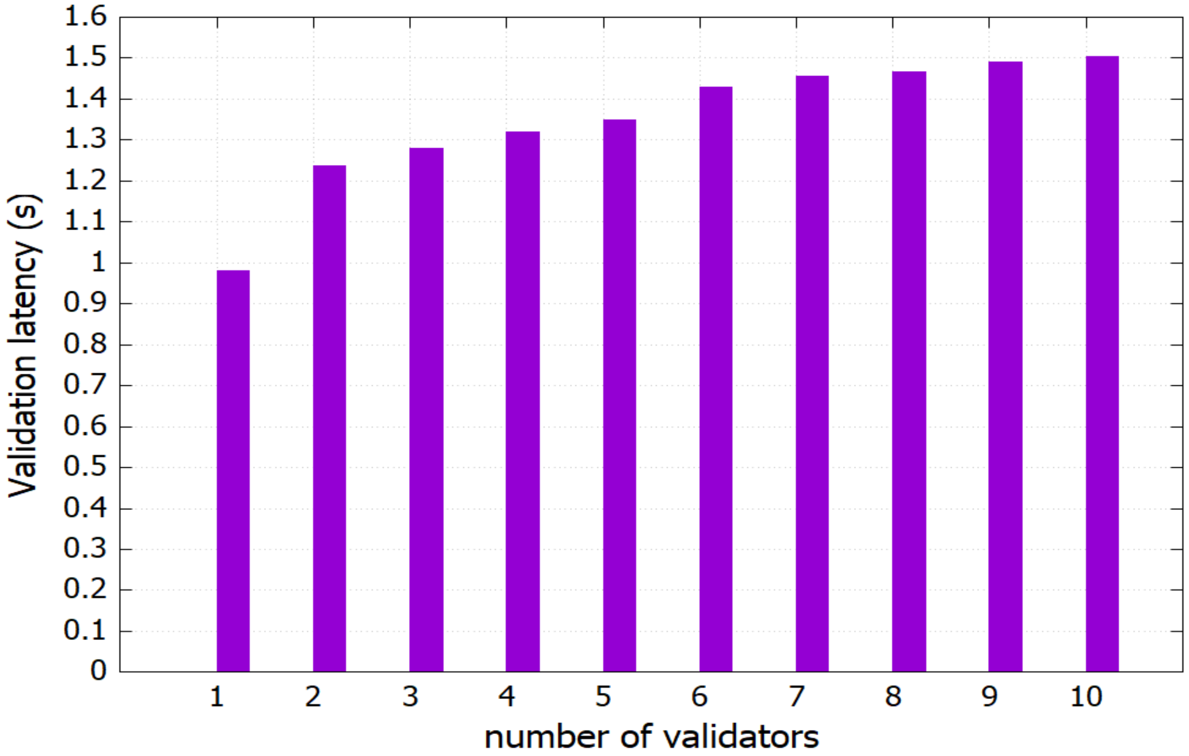
Settings & test environment

- Blockchain: Tendermint plateform (https://docs.tendermint.com/)
- 10 Docker containers that act as brokers and validator nodes
- Cryptographic tools: PBC pairing library (https://crypto.stanford.edu/pbc/download.html)

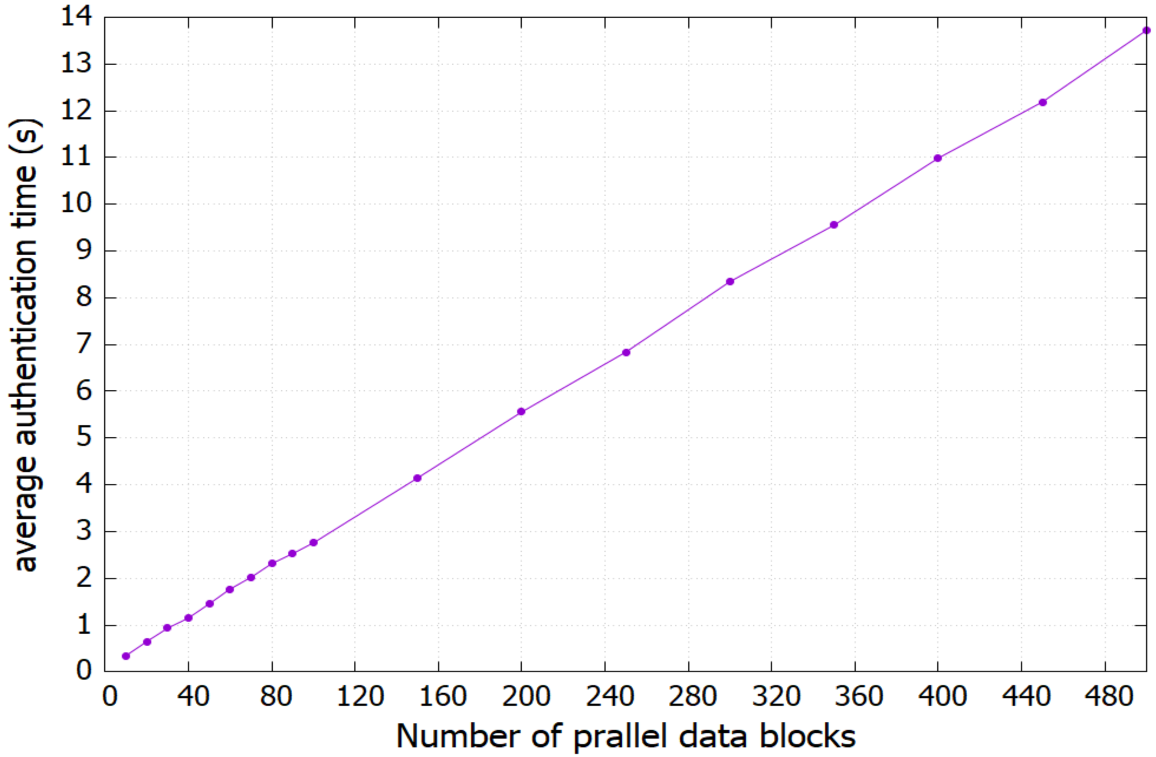




Blockchain layer: impact of transactions rate and number of validator nodes



Validation latency w.r.t. transactions rate



Validation latency w.r.t. the number of validators

7. Conclusion and perspectives

7.1 Conclusion and perspectives

- We proposed an anonymous Blockchain-based data sharing protocol for VANETs
- Our results are promising and show that blockchain can leverage security and privacy in IoT applications

As perspectives, we intend to:

- Investigate other efficient anonymization techniques like l-diversity and differential privacy techniques in VANETs
- Address the problem of protection of vehicles' geolocations using “Gridding” techniques
- Investigate the privacy issues related to blockchain technology applied in the context of IoT (Zk-Snark techniques)

Thanks !

Publications

– International Journal publications

1. **Kouicem, D. E.,** Bouabdallah, A., & Hicham, L. (2018). *Internet of things security: A top-down survey*. Computer Networks, 141, 199-221.
2. **Kouicem, D. E.**, Imine, Y., Bouabdallah, A., Hicham, L. *Trust management based blockchain protocol for Internet of Things".* in IEEE Transaction on Dependable and Secure Computing. To appear

– International Conference publications

1. **Kouicem, D. E.**, Abdelmadjid, B., & Hicham, L. *Distributed Fine-Grained Secure Control of Smart Actuators in Internet of Things*. In 2017 IEEE ISPA (pp. 653-660).
2. Imine, Y., **Kouicem, D. E.**, Bouabdallah, A., & Ahmed, L. *MASFOG: An Efficient Mutual Authentication Scheme for Fog Computing Architecture*. In 17th IEEE Trustcom, 2018.
3. **Kouicem, D. E.**, Bouabdallah, A., Hicham, L. *An Efficient Architecture for Trust Management in IoE Based Systems of Systems*. In the 13th IEEE SoSE, 2018.
4. **Kouicem, D. E.,** Bouabdallah, A., Hicham, L. *An Efficient and Anonymous Blockchain-Based Data Sharing Scheme for Vehicular Networks*. In the 25th IEEE ISCC.
5. I. Fajjari, N. Aitsaadi, **Kouicem DE.**. A Novel SDN Scheme for QoS Path Allocation in Wide Area Networks. In 2017 IEEE GLOBECOM 2017, Singapore, December 4-8, 2017.
6. **Kouicem DE.**, I. Fajjari, N. Aitsaadi. An enhanced Path Computation for Wide Area Networks based on Software Defined Networking. In 2017 IFIP/IEEE IM, Lisbon, Portugal, May 8-12, 2017