

A NEW APPROACH TO PKI: BLOCKCHAIN!

Emiliano, Orrù | Manager | em.orrù@reply.it

Fabio, Vallone | Senior Consultant | f.vallone@reply.it

WHO ARE WE?

Spike Reply!



Emiliano Orrù

Manager @ Spike

Head of Mobility and Trust business units. Several years of experience in cybersecurity project on Automotive and Manufacturing sectors



Fabio Vallone

Senior Consultant @ Spike

Cybersecurity Expert with several years of hands-on experience on Cryptography, Automotive Security (ISO 21434, R155/6) and Offensive Security in large Enterprises



MEETING AGENDA

A NEW PKI APPROACH: BLOCKCHAIN!

- 1 Introduction
- 2 PKI use cases
- 3 A new approach!



INTRODUCTION

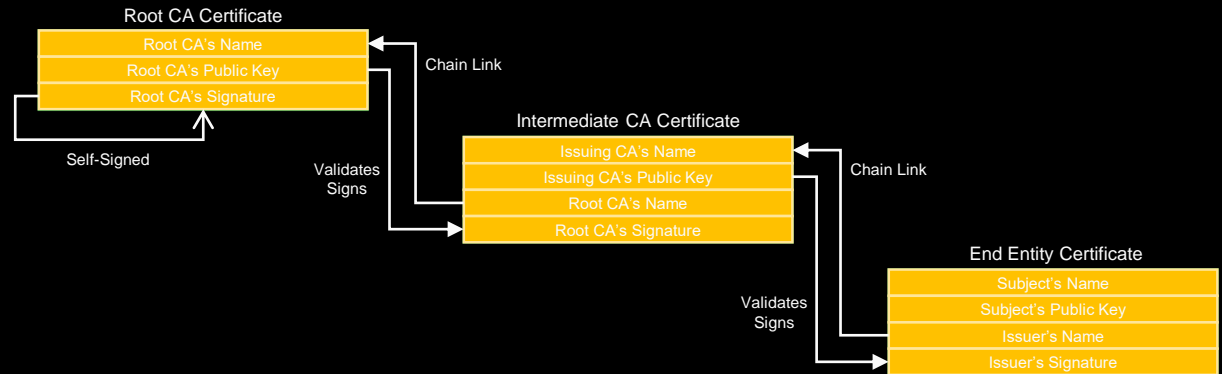


PUBLIC KEY INFRASTRUCTURE

INTRODUCTION

A Public Key Infrastructure (PKI) is a combination of policies, procedures and technologies needed to manage digital certificates.

It is the foundation that enables a safe use of asymmetric encryption and of digital signatures.



PUBLIC KEY INFRASTRUCTURE

USE CASES



Machine to
Machine
interaction,
Secure
Communic
ation



Protection
of the
Identity



Protection
of the SW



V2X, IoT



A NEW APPROACH: BLOCKCHAIN!

Spike Reply has created a PoC regarding a PKI based on a Blockchain.

The work has been done in collaboration with PoliTo as a Master Degree thesis work¹

The PoC starts from the research carried out by M. Toorani and C. Gehrman at the Swedish Lund University², who proposed a general model to create a distributed PKI based on blockchain.

1. <https://webthesis.biblio.polito.it/24600/>
2. <https://portal.research.lu.se/en/publications/a-decentralized-dynamic-pki-based-on-blockchain>



BLOCKCHAIN PKI!



WHAT IS A BLOCKCHAIN

KEY CONCEPTS



TRANSACTION

Generally speaking is an exchange of assets between two or more parties. In the context of the Blockchain can be referred as the set of data that we want to certify.



NODE

Devices that participates in the Blockchain, on which runs the software of the Blockchain. Has the primary function to maintain the consensus by validating the transaction



CONSENSUS MECHANISM

Algorithm used by the Blockchain to reach the consensus and validate the transaction



IMMUTABILITY

Once a transaction is inserted inside a Blockchain it cannot be manipulated, replaced or falsified

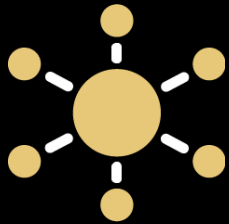


WHAT IS A BLOCKCHAIN

HOW IT WORKS



A new transaction is created



The transaction is then transmitted to a network of nodes which verify it



The network validates the new transaction



Once confirmed to be legitimate, the transaction is clustered into a block, with other transactions



The new block is then chained together with the last one






A NEW APPROACH

NODE TYPES

A node is represented by a running process **associated to** an asymmetric **key pair**.

Each node has a role among:

- **Root (R)** 
- **Intermediate (I)** 
- **Ordinary (O)** 

R and I nodes belong to the **consensus group**.

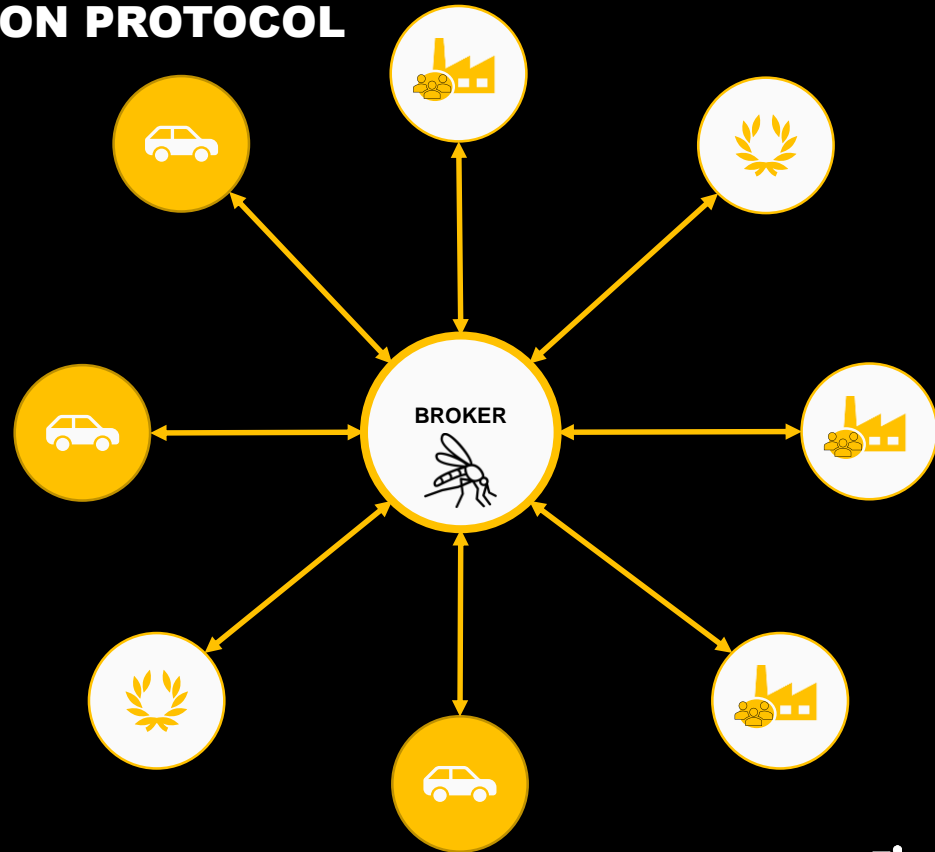


A NEW APPROACH

COMMUNICATION PROTOCOL

MQTT is a communication protocol based on the concepts of topic publication and subscription.

The broker coordinates all subscriptions and publications, making sure that each entity subscribed to a certain topic receives all the messages related to it.



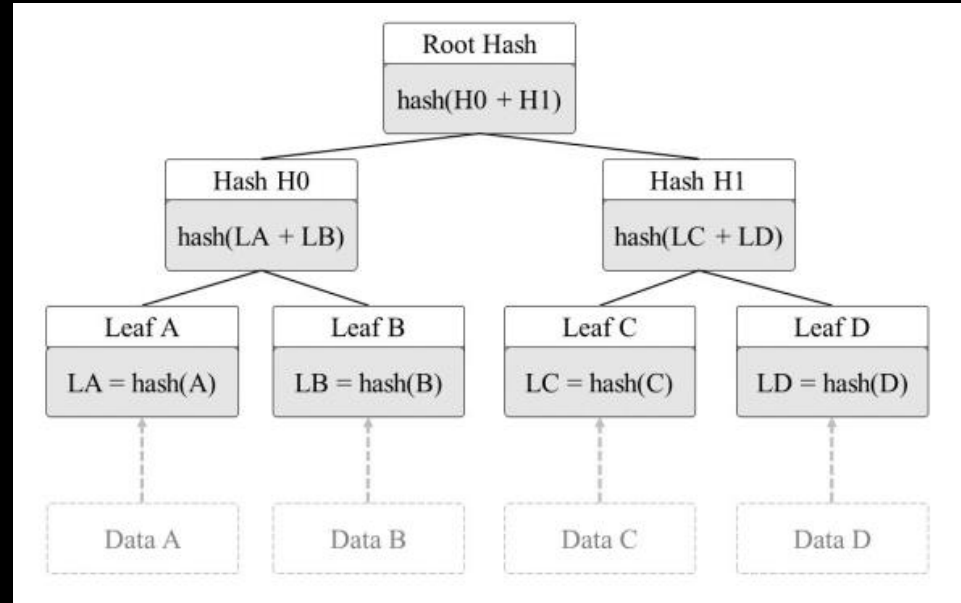
A NEW APPROACH

ACCUMULATOR

A **cryptographic accumulator** is a set of heuristics and polynomial-time algorithms **accumulating a finite set of items**.

For each of them, it provides a **witness ω** , which is a **proof of membership**, meaning that item has been accumulated.

Merkle Tree



A NEW APPROACH

PROCEDURES

It has been defined a set of procedures executable by nodes in order to create new blocks, or to verify validity of a certain public key.

Procedures are:

- **Enroll**: it can be used by R or I to create a new node;
- **Update**: updates the public key value of an entity;
- **Revoke**: revokes public key of an entity;
- **Verify**: verifies whether or not a public key is valid.



A NEW APPROACH

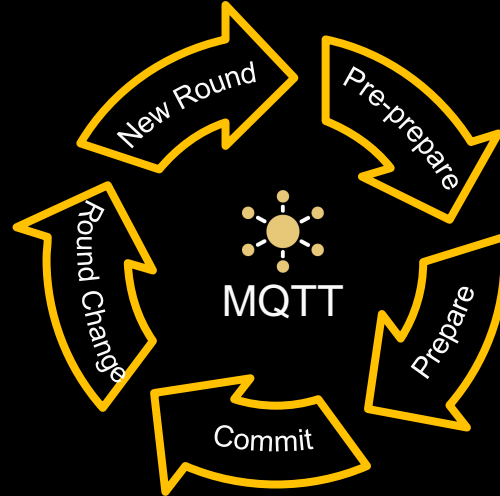
CONSENSUS MECHANISM: PBFT

New round

- Leader node impersonation
- Operation selection

Round Change

- Control left to UI
- System gets ready for next round



Commit

- Check of prepare messages
- If enough approvals → Commit to blockchain
- Else → Failure

Pre-prepare

- New block proposal
- Signed multicast pre-prepare message to all validators

Prepare

- Validators check leader's proposal
- Approval / Rejection carried by prepare messages



A NEW APPROACH

TRUST WEIGHTS

- Initial value depending on role type
- Weighted on time
- Reward-and-punishment mechanism



Commit successful if threshold

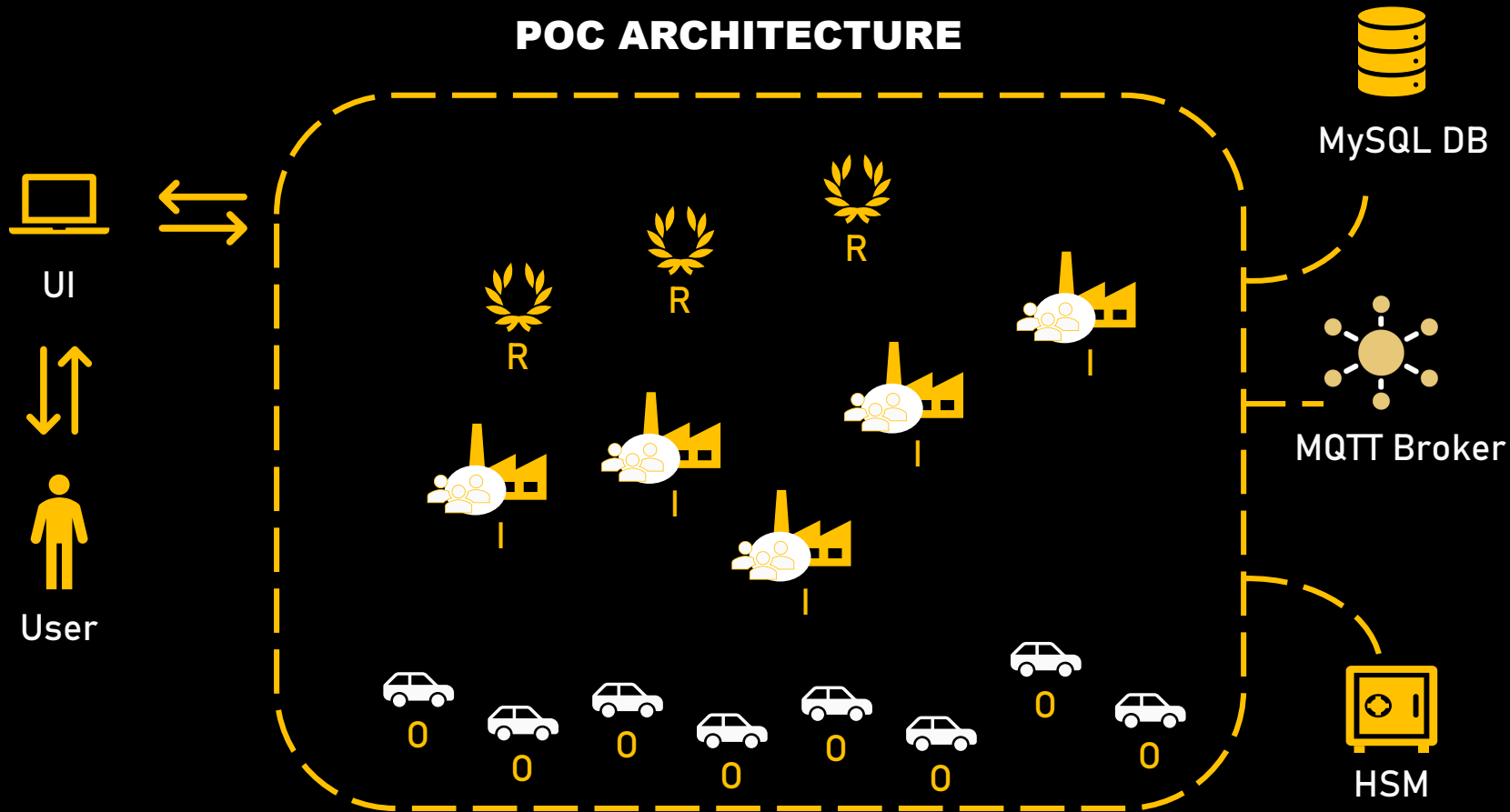
$$T = (2[t - 1] + 1) \cdot \omega_{avg}^i$$

is reached



A NEW APPROACH

POC ARCHITECTURE



THANK YOU

www.reply.com

