Blockchain account authentication through x509 PKI

Adja Elloh Yves Christian
elloh.adja@epita.fr

Sécurité Systèmes -LRE

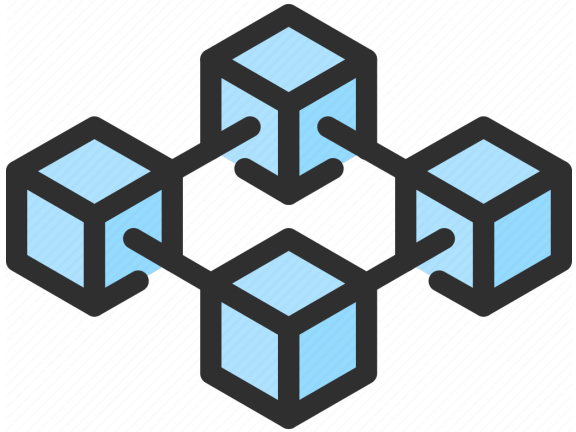
July 1, 2023

Table of Contents

The Blockchain

The Blockchain

- **Is a distributed system**
  - based on peer to peer network model
- **High level of transparency**
  - Hard to tamper
- **Is pseudonym**
  - based on pseudonym accounting



Blockchain

System ensuring secure data exchange between peers

- Network of users
  - Sharing a ledger
- Public, permissioned or private system
- Relying on a consensus system

Blockchain Users

Two types of users:

Validators

- are users responsible for validating new transactions and maintaining the security of the Blockchain
- They store usually the entire Blockchain

Simple user

- These are users who come to take advantage of Blockchain services

Blockchain Entities

Two types of Entity:

- External account (EOA)
  - Owned by a physical user
  - Managed through a wallet

- Internal account (Contract)
  - Created and managed by an external account
  - Governed by rules contained in the smart-contract code

Blockchain accounting

An account is needed for every interaction with the Blockchain

- Account is managed with a keypair
  - Public / private key
- Identified through an hex ID
- Is public

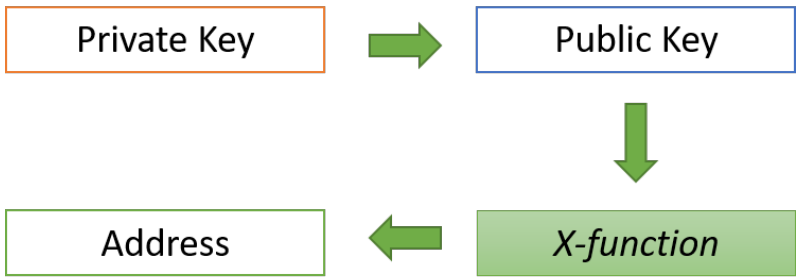


Table of Contents

Blockchain challenges

- Blockchain is a hostile environment, mistrust is the basis
- The anonymity of users must be guaranteed
- Is public
- It is decentralized

Authentication methods

Available solution

- Passphrase
  - Used for users authentication in wallet
  - The passphrase must be protected in a safe box
- Symmetric cryptography
  - Not used in Blockchain architecture
  - needs a key exchange
- Signature
  - Used for transaction validation
  - Authenticates the link to belong to a public key
- Certificate
  - Useful but require a PKI
  - Very complicated to use
- ...

Table of Contents

The Public key infrastructure (PKI x509)

The PKI is one of the security architecture proposed to ensure security primitives and services.
The PKIx architecture (e.g used for traditional internet) is composed of:

- Certificate authority (CA)
  - that stores, issues and signs the digital certificates
- Registration authority (RA)
  - which verifies the identity of entities requesting digital

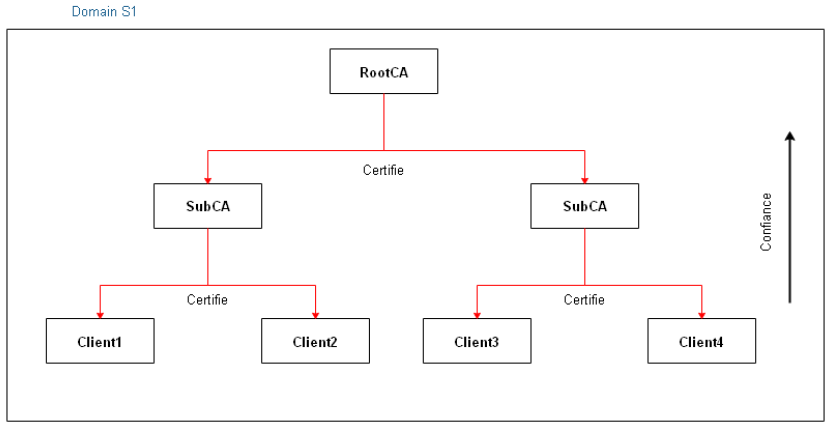
The Public key infrastructure (PKI x509)

- CRL ISSUER
  - a system that generates and signs CRLs
- REPOSITORY
  - a system or collection of distributed systems that stores certificates and CRLs and serves as a means of distributing these certificates and CRLs to end entities.

The Public key infrastructure (PKI x509): Trust model

Trust models

- Hierarchical
- Network (web of trust)
- ...



X509 PKI (PKIX)

- It is the dominant PKI in the internet
- Several entities including users of the Blockchain have x509 certificates
- It is a standard and it is customizable (X509 extensions)
- Able to take into account any encryption algorithm

X509 PKI (PKIX)

Not suitable for total use in the Blcokchain ecosystem

- Because it binds personal information to a key pair
- The trust models are not adapted
- Revocation is complicated
- the certificate is heavy (too much information)

PKIX usecases

There are certain cases where its use can be interesting

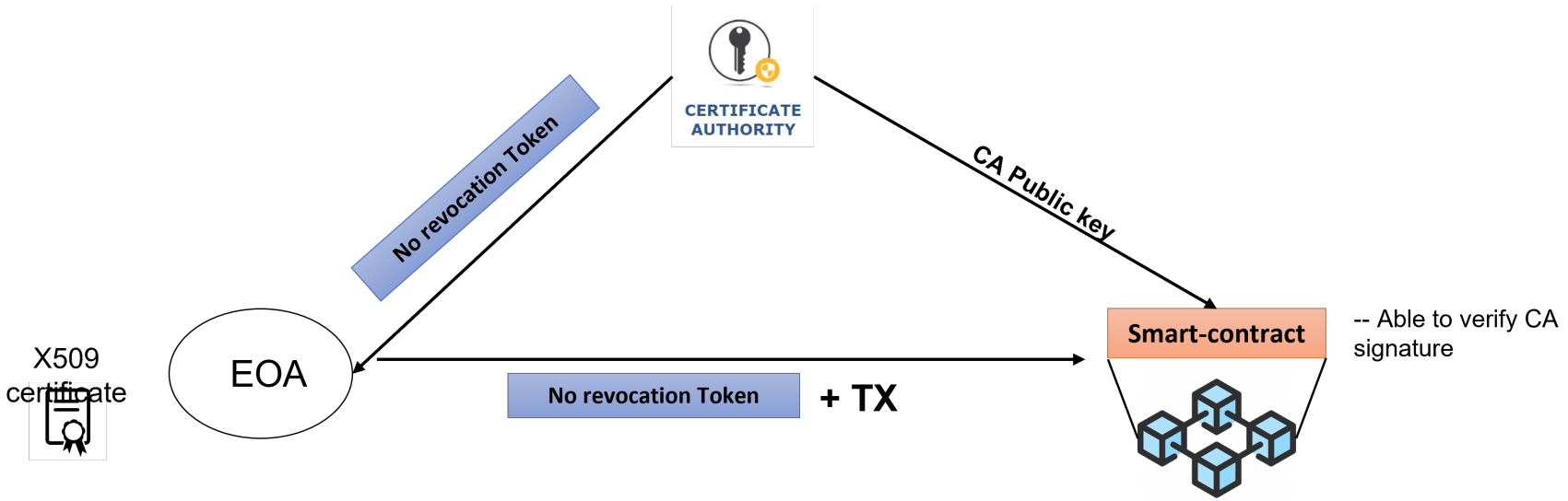
- When questions of anonymity and traceability do not arise
- when the entity already uses PKI services
- When CAs are shared
- When the problem of certificate revocation is solved
- ...

Table of Contents

PKIX usecases

Authentication of external accounts with smart-contracts

- X509 extension
- No revocation token
- Encryption algorithm
- Time definition



References I

- https://datatracker.ietf.org/doc/html/rfc4033
- https://www.internetsociety.org/deploy360/dnssec/tools/
- https://www.icann.org/resources/pages/dnssec-what-is-it-why-important-2019-03-20-fr
- https://www.infoblox.com/glossary/dns-over-tls-dot/
- https://datatracker.ietf.org/doc/html/rfc7858
- Deep Packet Inspection, Jens Myrup Pedersen, Aalborg University
- https://www.akamai.com/fr/our-thinking/cdn/what-is-a-cdn
- https://www.avast.com/fr-fr/c-what-is-a-vpn