

Merging Metrological Digital Artefacts with Blockchain

Universidade Federal de Santa Catarina (UFSC)
Laboratório de Segurança em Computação (LabSEC)



INMETRO Digital Metrology - ICP-Brasil

- INMETRO has a digital certification for metrology project
- Became a Certification Authority for ICP-Brasil in 2022
- Implementation of the fuel pump digital signature verification system developed by INMETRO
- Development of an application for citizens to monitor fuel supply fraud
- Security and inspection infrastructure

< Informações da Bomba

Medida Inteligente

 **Dados do estabelecimento**

Razão Social: UFSC
Endereço: CAMPUS UNIVERSITÁRIO REITOR JOÃO DAVID FERREIRA LIMA 88.040-970, Florianópolis, SC

 **Dados do abastecimento**

Número de série do instrumento: 1
Indicador: 1
Data: 20/1/2022
Hora: 10:51:17
Volume abastecido: 10,2L
Preço/litro: R\$5,329
Total a pagar: R\$54,356



Assinatura digital válida.

[Relatar Problema](#) [Mais Informações](#)

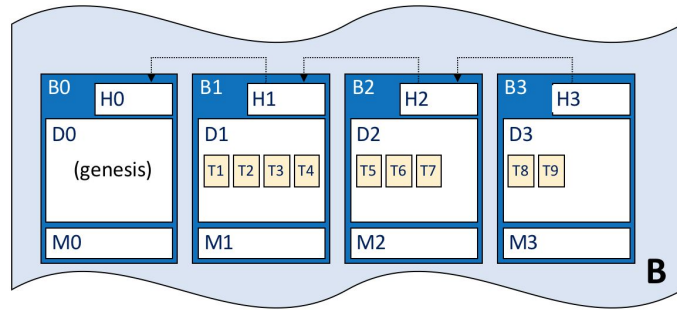
 [Nova Leitura](#)








INMETRO Digital Metrology - Opportunity

- Every metrological device will be able in the future to generate digitally signed receipts of measure
- We can track use and calibration
- If we collect all the measures we can derive by products:
 - Fuel pumps:
 - Actual car efficiency certification results
- The question is:
 - How to collect?
 - How to organise?
 - and how to process?

Hyperledger Fabric - Ledger

- Storage:
 - Ledger:
 - Transaction list.
 - Block chaining (History);
 - Pointer(Hash);
 - World State:
 - (Key, Value);
 - Most recent state;
 - Private and Permissioned.



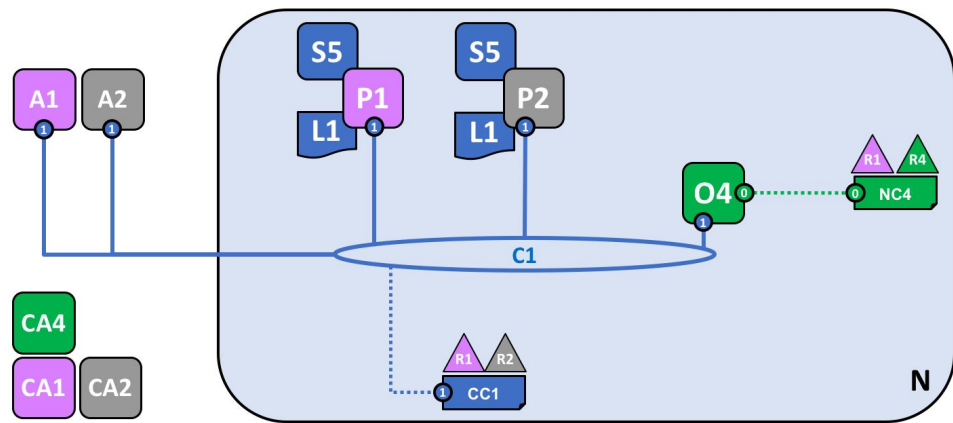
	Blockchain
	Block
	Block header
	Block data
	Transaction
	Block metadata
	H2 is chained to H1

Fonte: <https://hyperledger-fabric.readthedocs.io/en/release-2.2/ledger/ledger.html>



Hyperledger Fabric - Network Organization

- Organizations (R's)
- Computers (O4)
 - Network configuration (NC4)
- Channels (C1)
 - Channel configuration (CC1)
- Peers (P's) with ledgers (L1) and smart contracts (S5)
- Applications (A1)
- Certificate Authorities (CA's)



Fonte: <https://hyperledger-fabric.readthedocs.io/en/release-2.2/network/network.html>



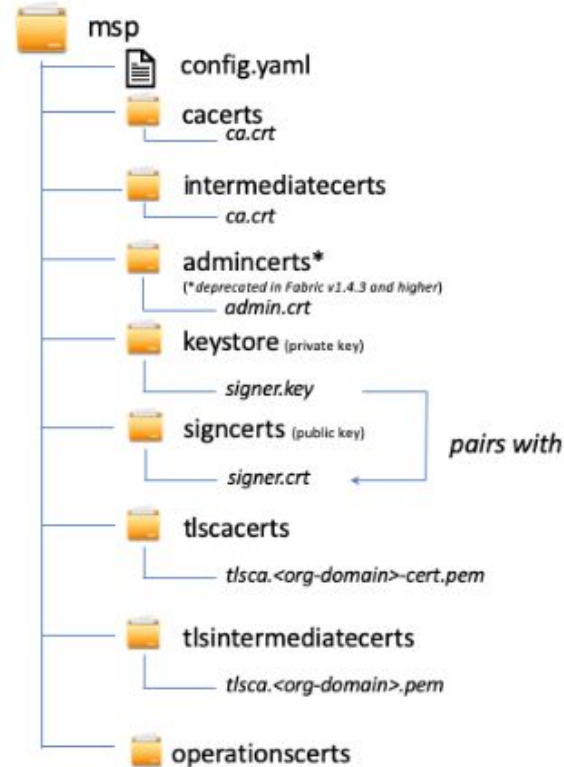
Hyperledger Fabric - Identities

- Entities are identified by X.509 certificates or aliases
- Mostly by certificates
- Certificates issued by organization CA or intermediate CA
- Different certificate fields identify an entity
- Ideal for government solutions because it does not assume pseudo-anonymity by default.



Hyperledger Fabric - Membership Service Provider (MSP)

- Set of folders that define an organization's identities
- Folders contain certificates or keys



Hyperledger Fabric - Certificate Standard

- The important certificate fields for the Fabric network are: OU, CN and OID
1.2.3.4.5.6.7.8.1
- OU: identifies the role of the entity
- CN: the name of the entity
- OID: stores attributes related to the invocation of smart contracts
(chaincodes)

```
NodeOUs:  
  Enable: true  
  ClientOUIdentifier:  
    OrganizationalUnitIdentifier: client  
  PeerOUIdentifier:  
    OrganizationalUnitIdentifier: peer  
  AdminOUIdentifier:  
    OrganizationalUnitIdentifier: admin  
  OrdererOUIdentifier:  
    OrganizationalUnitIdentifier: orderer
```

```
1.2.3.4.5.6.7.8.1:  
  {"attrs":{"energy.seller":"true","hf.Affiliation":"ufsc","hf.EnrollmentID":"seller1-ufsc","hf.Type":"client"}}
```



Hyperledger Fabric - Integration with ICP-Brasil

- Default on Hyperledger Fabric:
 - X.509 certificates;
 - Organizational Unit (OU):
 - Organization of the MSP;
 - Policies;
 - ECDSA NIST Keys:
 - P224; P256; P384; P521.
- Change proposals:
 - Removed NIST Curves: DOC-ICP-01.01
 - EdDSA Keys:
 - Ed25519;
 - Ed448.
- Merge Request (MR) for Hyperledger Fabric;
- New Edwards CAs and/or Existing CAs.

Geração de Chaves Assimétricas de AC	
Normativo ICP-Brasil	DOC-ICP-01 - item 6.1.1.3 DOC-ICP-04 - item 6.1.1.3 DOC-ICP-01 - item 6.1.5 DOC-ICP-05 - item 6.1.5
Algoritmo	RSA ou ECC-Brainpool (conforme RFC 5639) ou Ed448-Goldilocks (PureEdDSA e HashEdDSA, conforme RFC 8032) ou E-521 (Conforme parâmetros da curva estabelecidos neste DOC-ICP-01.01, PureEdDSA e HashEdDSA, conforme RFC 8032).
Tamanho de chave	RSA 4096 ou brainpoolP512r1 ou Ed448 (448 bits) ou E-521 (521 bits).
Geração de Chaves Assimétricas de Usuário Final	
Normativo ICP-Brasil	DOC-ICP-04 - item 6.1.5.2
Algoritmo	RSA ou ECC-Brainpool (conforme RFC 5639) ou Curve25519 (Conforme RFC 7748) ou Ed25519 (PureEdDSA e HashEdDSA, conforme RFC 8032) ou Ed448-Goldilocks (PureEdDSA e HashEdDSA, conforme RFC 8032) ou E-521 (Conforme parâmetros da curva estabelecidos neste DOC-ICP-01.01, PureEdDSA e HashEdDSA, conforme RFC 8032).
Tamanho de chave A1, A2, A3, A CF-e-SAT, S1, S2, S3, T3, OM-BR	RSA 2048 ou brainpoolP256r1 ou Curve25519 (256 bits) ou Ed25519 (256 bits) ou Ed448 (448 bits) ou E-521 (521 bits)
Tamanho da chave A4, S4, T4	RSA 2048 ou RSA 4096 ou brainpoolP512r1 ou Curve25519 (256 bits) ou Ed25519 (256 bits) ou Ed448 (448 bits) ou E-521 (521 bits)



Hyperledger Fabric - Certificate Standards (Algorithms)

- In the current version (2.4.6) entities sign with an ECDSA certificate
- AC's can use ECDSA or RSA
- We produce Edwards curve support (ed25519)
- PR: Add ed25519 support #3343
 - Likely native support in 3.0

Add ed25519 support #3343
johannww wants to merge 22 commits into `hyperledger:main` from `johannwi:ed25519-support`

johannww on 15 Aug
I am evaluating a possible solution, as I believe these requirements will lead to changes in the Signer interface
<https://github.com/johannww/fabric-1/blob/9fdc4f0c3ac92a7c95ab0099ac6535a1fc4410f0/bccsp/signer/signer.go#L76-L78>
So functions like the one below can be called:
<https://github.com/johannww/fabric-1/blob/9fdc4f0c3ac92a7c95ab0099ac6535a1fc4410f0/msp/identities.go#L255-L278>

johannww 16 days ago
I think it is fixed. Plus, I forced-pushed some commits because they were not signed off.

C0rWin and others added 10 commits 16 days ago

- Use actual address of the deadMembers2Expire slice variable (`hyperled...`) 6dce9eb
- Bump zap-logfmt ... 2961272
- Handle empty policies when traversing the policy tree in discovery po... 34bc86f
- Add ed25519 support ... 735ed9e
- Add initial integration tests for ed25519 ... 2d1e290
- Add ed25519 channel and msp capabilities ... 758e0ba
- Enhance capabilities and add ed25519 integration tests ... 672987c
- Delete integration/ed25519 folder and revert vendor file ... bf1382c
- Update Channel capabilities and msp version to V3_0 ... 5398a74
- Remove Ed25519 standard network ... ff0e6e4

johannww added 12 commits 16 days ago

- Remove oldPeerRunner from integration test net ... 1bcadd...



Proposal

- Our proposal is for the creation of a blockchain of metrological receipts
- Tracking use and possibly calibration
- Devising new strategies for regulator when using calibrated and connected devices
 - Fuel pumps:
 - Tax avoidance
 - Indications on problems with mixtures
- Combination of on-chain and off-chain information

Thank you!



References

- A Blockchain Platform for the Enterprise - Hyperledger Fabric. Link: <https://hyperledger-fabric.readthedocs.io/en/latest/index.html>. Acesso: 14/09/2022;
- Instituto Nacional de Tecnologia da Informação - Documentos Principais. Link: <https://www.gov.br/iti/pt-br/assuntos/legislacao/documentos-principais>. Acesso: 14/09/2022;

