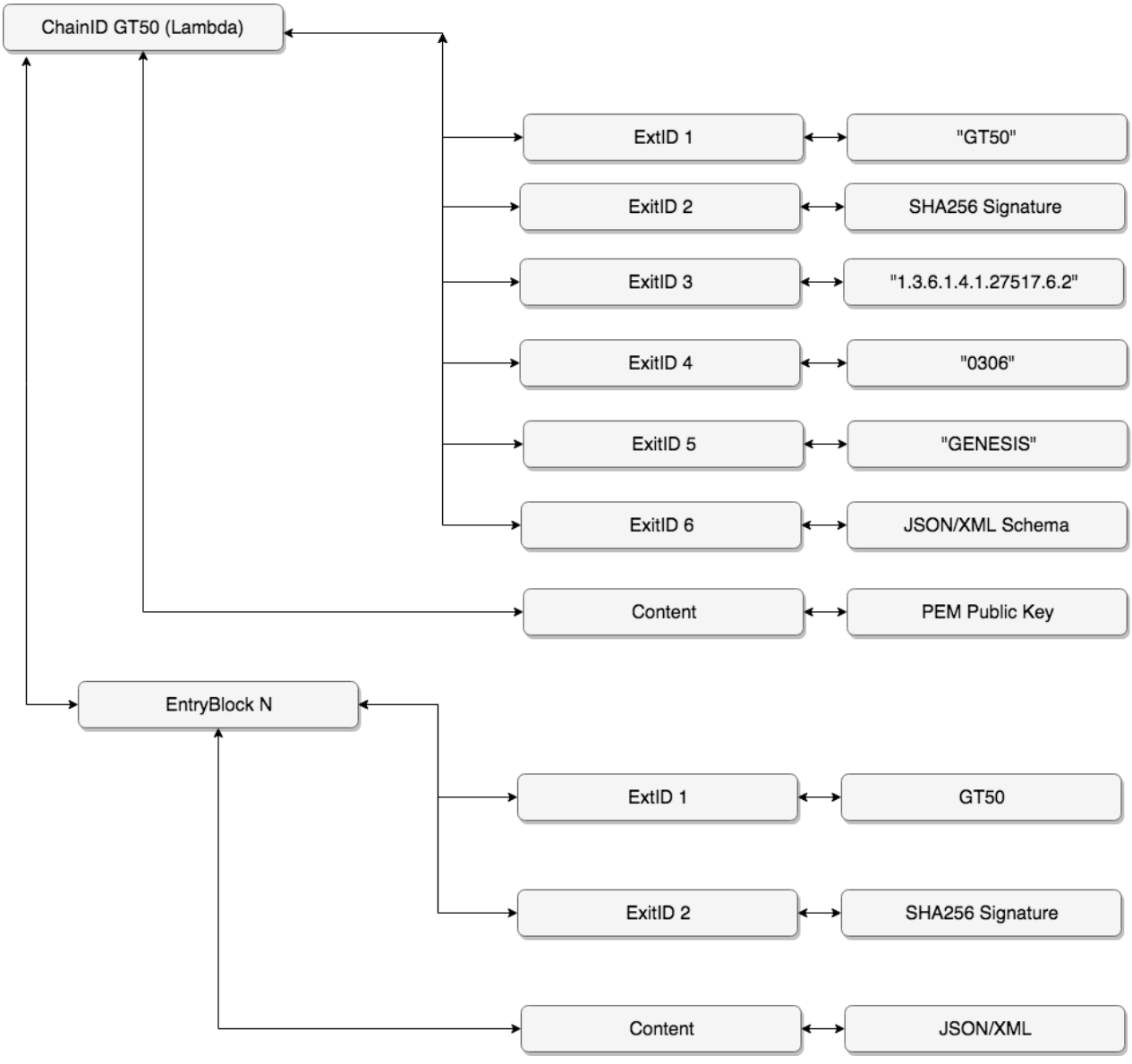
Guida alla verifica dei dati presenti nella BlockChain FACTOM

Questa documento vi guiderà alla verifica autonoma dei dati inseriti dal servizio Lambda all'interno della BlockChain FACTOM. Se infatti l'opzione per la BlockChain FACTOM è stata attivata, ad ogni caricamento all'interno del LambdaStore tramite l'Applicazione LambdaSign, verranno inserti dei metadati per identificare univocamente il documento inserito in un blocco facente parte della catena (ChainID) che GT50 ha "riservato" per questa applicazione.

Per una descrizione generica del servizio Lambda si veda:

https://www.gt50.org/products/IT/lambdaservice/

Di seguito uno schema che riassume i dati inseriti nella BlockChain FACTOM:



I dati sono così inseriti:

- ChainID: blocco di riferimento "GENESIS" assegnato a GT50 sotto cui verranno inseriti tutti i successivi EntryBlock dei diversi documenti degli utenti (un EntryBlock per documento). Il Content del relativo blocco è la chiave pubblica codificata in BASE64 con cui verranno firmati tutti i metadati dei documenti successivi. Questo garantisce che i dati inseriti siano stati firmati solo e soltanto dalla chiave privata di GT50.
- Singolo EntryBlock: contiene i metadati del file PDF presente in LambdaStore in formato JSON. Il campo *ExtID 2* è la firma SHA256 del contenuto firmato tramite la chiave privata GT50 che ne garantiche l'autenticità. *ExtID 1* è una semplice etichetta con la scritta "GT50" per identificare velocemente il blocco.
    - Nello specifico il contenuto JSON è così formato:

      `{ "Type": "Data", "HashFile": "6448534DCF2B763AADE04D9439E3D9192F36C15E294318F038FD8750F531D7EC", "HashFilePADES": "87C98609BCB163DF1EA87E3E3A42BD1921AC7CB0734A2610B0687EB356B1443E", "DateTime": "20190206102558" }`
    - Type: identifica la possibile tipologia di dati.
    - HashFile: SHA256 del file originario prima della sua firma.
    - HashFilePADES: SHA256 del file firmato in formato PADES (Questo campo identificativo è la vera e propria impronta digitale del file che si è inserito in maniera completamente codificata nel LambdaStore).
    - DataTime: Data ora e minuti di creazione del file (unito al precedente campo HashFile identifica univocamente il file sul sistema Lambda Service) fornito dal client durante caricamento.

Tramite l'uso dell'App UniversalQReader si otterrà un messaggio di questo tipo:

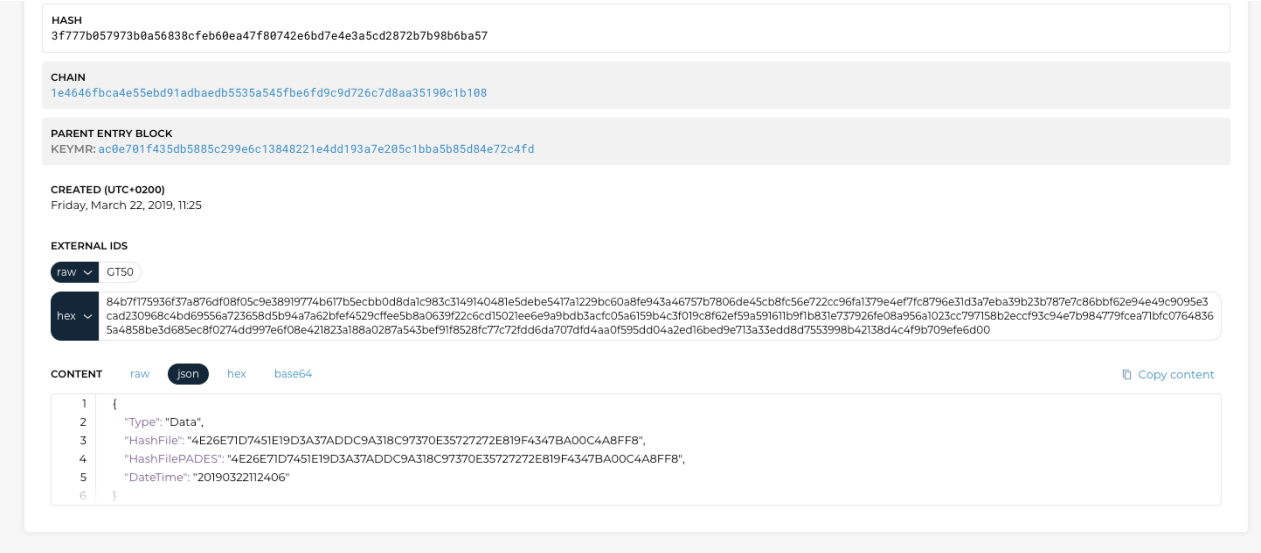
[ITA] I dati identificativi del documento sono inseriti nella BlockChain FACTOM con riferimento:

Link: https://explorer.factom.com/chains/1e4646fbca4e55ebd91adbaedb5535a545fbe6fd9c9d726c7d8aa35190c1b108/entries/3f777b057973b0a56838cfeb60ea47f80742e6bd7e4e3a5cd2872b7b98b6ba57

[ENG] The document identification data is entered in the FACTOM BlockChain with reference:

Link: https://explorer.factom.com/chains/1e4646fbca4e55ebd91adbaedb5535a545fbe6fd9c9d726c7d8aa35190c1b108/entries/3f777b057973b0a56838cfeb60ea47f80742e6bd7e4e3a5cd2872b7b98b6ba57

Cliccando si verrà reindirizzati al sito Explorer messo a disposizione da FACTOM per la lettura di tutti i blocchi presenti in FACTOM come da esempio:



Verifica diretta del file PDF scaricato tramite il client UnivesalQReader

1) Decodifica del QRCode presente sul documento in vostro possesso tramite l'App UniversalQReader.

2) Salvataggio del documento in formato PDF PADES per la verifica successiva.

3) Calcolo dello SHA256 del file PADES scaricato tramite l'App UniversalQReader (ad esempio utilizzando il sito: https://emn178.github.io/online-tools/sha256_checksum.html).

4) Lo SHA256 da voi calcolato in modo autonomo, dovra' essere confrontato con quanto indicato in "Content ⟶ HashFilePADES": se i due valori sono identici, avrete la conferma che il file che avete scaricato tramite l'App e' stato notarizzato con l'inserimento dei suoi dati nella blockchain FACTOM.

Verifica dei dati JSON tramite la firma presente nell'EntryHash del documento in FACTOM

La verifica precedente garantisce che il file scaricato sia effettivamente il file firmato dall'Utente i cui metadati sono stati poi inseriti nella BlockChain. E' necessario attuare un'ulteriore verifica che garantisca tuttavia che i dati riportati nel blocco siano a loro volta firmati con la chiave privata di GT50. Se la verifica è positiva possiamo così essere sicuri che i dati presenti in BlockChain siano stati realmente inseriti dal servizio Lambda Service: la blockchain e' pubblica e chiunque potrebbe aggiungere dati non corretti. La firma digitale di GT50 garantisce la possibilita' di verificare la correttezza di questi dati.

Per effettuare la verifica della firma digitale della Entry che vogliamo controllare, seguire la procedura riportata:

1) Selezionare il campo *ExtID 2* in formato Base64.

2) Trasformare il dato dal formato Base64 (**base64 --decode**) in una sequenza binaria, quindi salvarlo in un file (es: signature.dat).

3) Prelevare dal blocco genesis della ChainID GT50/Lambda il campo Content⟶PEMPublicKey in formato BASE64 che contiene la chiave pubblica di GT50 con cui sono stati firmati tutti i successivi dati dei blocchi in FACTOM.

4) Trasformare il dato dal formato Base64 (**base64 --decode**) in una sequenza binaria, quindi salvarlo in un file (es: *public_key.pem*) .

5) Utilizzare questo semplice codice di verifica in PHP:

```
<?php
//data you want to verify
$data =
'{"Type":"Data","HashFile":"4E26E71D7451E19D3A37ADDC9A318C97370E35727272E819F4
347BA00C4A8FF8","HashFilePADES":"4E26E71D7451E19D3A37ADDC9A318C97370E35727272E
819F4347BA00C4A8FF8","DateTime":"20190322112406"}';
file_get_contents('public_key.pem', $public_key_pem);
file_get_contents('signature.dat', $signature);
//verify signature
$r = openssl_verify($data, $signature, $public_key_pem,
"sha256WithRSAEncryption");
var_dump($r);`
?>
```

6) Oppure a linea di comando usando la libreria OpenSSL (https://www.openssl.org/): *openssl dgst -sha256 -verify public_key.pem -signature signature.dat "{"Type":"Data","HashFile":"4E26E71D7451E19D3A37ADDC9A318C97370E35727272E819F4347BA00C4A8FF8","HashFilePADES":"4E26E71D7451E19D3A37ADDC9A318C97370E35727272E819F4347BA00C4A8FF8","DateTime":"20190322112406"}"'*

7) Gli esempi riportati NON devono ovviamente ritonare errori di alcun genere relativi alla firma.