EN Blockchain OFF-Chain Concept

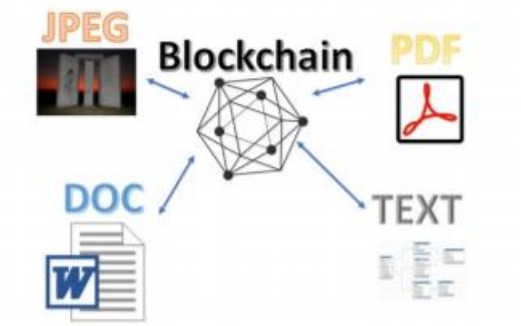
Zeljko Milinovic, MSc – Certified Blockchain Architect

Blockchain is not intended to store large amount of data. The Hyperledger Private Data Collection togehter with CouchDB (SideDB) reads the submitted data from the Ledger and creates a state for itself. This CouchDB state will allow us to create rich queris for complex searchs of the Ledger and is natively included in the Fabric. The states of the Couch Database are being refreshed constantly troughout the lifecycle of the Ledger.

As Blockchain is not a silo application and also no Data Warehouse database. The files needed in the case/incident workflows of Enduring Net, need to be stored.

We have also design issues concerning scalability of the blockchain like the limited size of it's blocks. What makes it impossible to store more complex data than transaction history, registry entries, and hashes in a block.

To resolve the issue the Enduring Net will adapt the usafe of IPFS for Off-Chain storage.



IPFS a versatile and extensible decentralized file system. After IPFs integration with Hyperledger and CouchDB, it becomes possible store only the hash data on-chain. The data itself will be stored off-chain, in IPFS.

The hash of a file fully corresponds to the content loaded into IPFS and is actually, in itself, the content address. If the file is modified, its hash will change and the file will no longer be available at the same content address. This makes it impossible for third-parties to change the uploaded content, opening up many opportunities for practical application in the fields of transmission and storage of reliable data.

A hash is a long number (think 256 bits, or around 80 decimal digits) which uniquely identifies a piece of data. The hash is calculated from the data using a one-way function which has an important cryptographic property: The hash is calculated from the data using a one-way function which has an important cryptographic propertyData hash associates with smart contracts, which organize the transaction cycle. This is another important feature of blockchain IPFS integration: Participants get the ability to control access to the data itself, including on an optional owner basis, without any intermediaries. The hash is encrypted with the private key of the recipient. This is a guarantee that only those who own will be able to gain access to the data.

An asymmetric encryption algorithm with public key is used to generate the signature that contains the hash address of the content and the password to decrypt the data blocks. The data blocks themselves are encrypted using the AES-256 symmetric algorithm, since the asymmetric encryption

algorithm is not efficient when it comes to working with large amounts of data in terms of performance and resource requirements when compared to symmetric.

Which data should be saved as Off-Chain in Enduring Net also to comply to GDPR Laws

Important to say that every User in the Blockchain has a cryptographicaly encrypted Blockchain wallet with his Identity. Hyperledger Indy will be also introduces as a Concept with DID and Soeverign Identity to comply with the GDPR Laws. Also the Zero Knowledge Proof concepts will be used.

In case of design of the EN Blockchain we can consider following rules:

- Personal data will be stored Off-Chain the link between the personal data and the Ledger will be hashed and cryptographicaly linked, with Ledger storing only the hash of the data. Personal data can include everything personal from the Subject (like Name and all GDPR defined personal details of the subject)
- Files of any types (PDF, Pictures, JSON, XML, Biometric Documents etc.) will be encrypted from the submitter side and stored Off-Chain in the decentralized file system.
- If the Use case of a particular organisatio needs to store chunks of personal data ON-Chain, Enduring Net will implement pseudonymization of data, where we would separate the attributes of the private subject to an off-chain information which is essential to re-identification
- Off-chain will be so programmed , that the links between off-chain file system and pseudo-data can be deleted every time, to comply with GDPR
- The data stored ON-Chain like Personal ID, Incident ID and Case ID will be indentified with an Unique Index troughout the complete lifecycle in the Ledger Audit Trail.
- Any GDPR Details about the Incident can be encrypted (with the private keys of the holder of the data) and the hash links can be stored Off-Chain. The registry transaction entries of these events will be stored in the Ledger Channels.

Identity policies safe-guarding the encryption keys will be defined in the Hyperledger Indy DID concept.