NFT AS A PROOF OF DIGITAL OWNERSHIP-REWARD SYSTEM INTEGRATED TO A SECURE DISTRIBUTED COMPUTING BLOCKCHAIN FRAMEWORK

By: **Asahi Cantu Moreno**

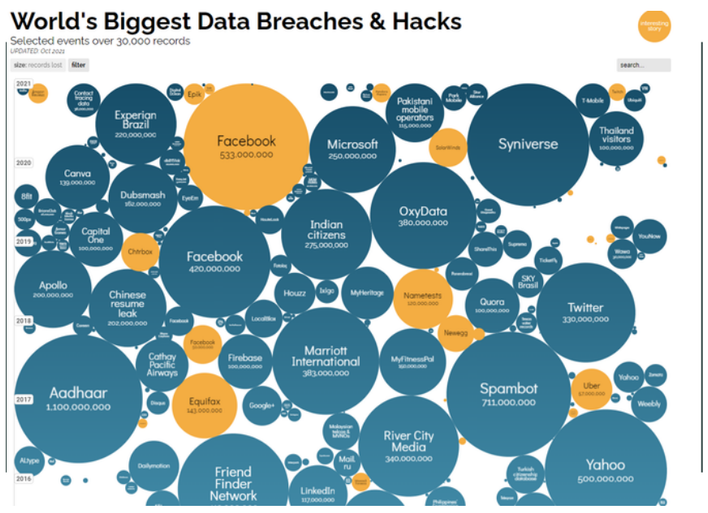
Universitetet i Stavanger

01 - INTRODUCTION

The industry is nowadays severely affected by security threats and cyber-attacks. Data and security breaches can cost enterprises and government institutions millions of dollars. The time-cost factor in changing a whole digital infrastructure is implausible to be confident enough information and systems remain compliant with the latest security standards.

HYPOTHESIS

The creation of a Blockchain-based system for industrial applications and data protection through NFTs and decentralized data storage systems make it possible to ensure data security while preserving system integrity.



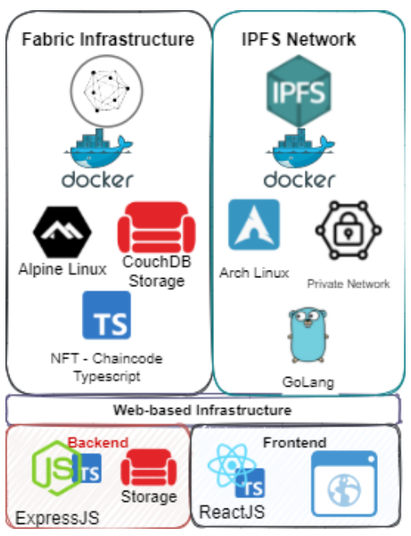
02 - OBJECTIVE

Propose a decentralized open-source web-based blockchain-based infrastructure that enables industries to securely share data and build up trust by the usage of a private IPFS network as a decentralized file system, smart contracts and NFT Technology (Non-Fungible Tokens-ERC-721 standard) with Hyperledger Fabric network and a web based system.

HYPERLEDGER FABRIC

IPFS

03 - METHODOLOGY



The project was created using open-source technologies:

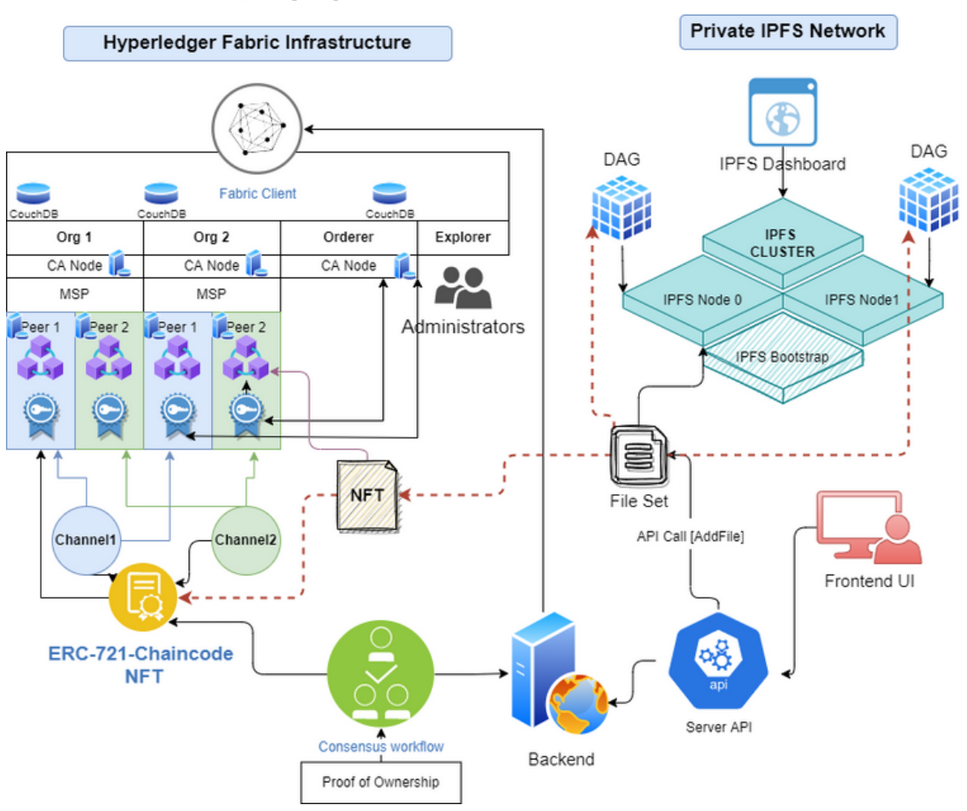
- **Hyperledger Fabric:** Permissioned blockchain infrastructure for industry applications.
- **Docker:** Virtualization technology used for microservice creation.
- **CouchDB:** Key-Value data storage system.
- **Typescript:** Programming language sitting as a superset of JavaScript.
- **IPFS.** Decentralized file system storage (private).
- **ArchLinux/Alpine Linux:** Linux OS distributions.
- **GoLang:** C-like compiled programming language.
- **ExpressJS:** Backend web application framework
- **React**: Open-source frontend library to build User Interface applications

05 - RESULTS

The NFT Blockchain-based system created the basis to demonstrate the plausibility of implementing an infrastructure for decentralized data governance in which multiple parties can interact with implicit trust. Implementing the adequate consensus mechanism, smart contract, and decentralized file system for data storage leverages cooperation and promotes fair participation by entities willing to manage data and be certified as asset owners. Treating information as a Non-Fungible token with the correct technology unleashes new ways of working and challenging security workflows with current centralized systems.

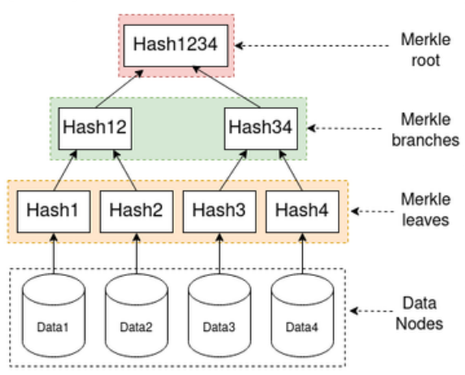
Since the solution is open-source and documented, it is possible to extend the functionality via smart contract extension and Backend/Frontend to be applied for other industries with specific business logic (food industry, real estate, music industry, health, use of NFT for royalties, tokenization, even IoT).

04 - ANALYSIS



- Permissioned Blockchain infrastructure
- Extended ERC-721 NFT Smart Contract
- Private IPFS Network
- REST API Server
- Client UI
- Proof of Ownership Consensus

MERKLE DIRECTED ACYCLIC GRAPH (DAG)



Organizations can join a private channel in the network with a trusted certificate and enroll users. Users can upload any data as NFT, then mint an NFT (which represents ownership). A unique ID (Hash) describes the content of the data and can be located in the IPFS network. Consensus mechanisms work to acknowledge authenticity and ownership of the user data. Other organizations can rank, endorse and acknowledge data ownership and relevance and. Users can transfer assets, amend data and add new version of it. System is **trustless**, decentralized and maintained by all organizations in the community.

~A Merkle tree is a relevant data structure in a blockchain system. It consists of a binary tree where each node stores the hash of its children nodes, and the root hash represents the hash of hashes. A single change in any node will drastically alter the root hash. This enables non-repudiation and trustability among systems.

Organizations can join a private channel in the network with a trusted certificate and enroll users. Users can upload any data as NFT, then mint an NFT (which represents ownership). A unique ID (Hash) describes the content of the data and can be located in the IPFS network. Consensus mechanisms work to acknowledge authenticity and ownership of the user data. Other organizations can rank, endorse and acknowledge data ownership and relevance and. Users can transfer assets, amend data and add new version of it. System is **trustless**, decentralized and maintained by all organizations in the community.

06 - CONCLUSION

Decentralized and Blockchain-based systems are relevant for the industry, its application can solve multiple security and trust-related problems. Shortly its implementation will be highly demanded. The NFT Technology began with digital technology, but its application and potential go far beyond. NFT and decentralized storage is key to building Web 3.0 and bringing society to a new era of cooperation, ownership, disruption, deconstruction, contribution, and reorganization.

RELATED LITERATURE

- Mengji Chen, Taj Malook, Ateeq Ur Rehman, Yar Muhammad, Mohammad Dahman Alshehri, Aamir Akbar, Muhammad Bilal, and Muazzam A. Khan. **Blockchain-enabled healthcare system for detection of diabetes.** Journal of Information Security and Applications, 58:102771, 2021. ISSN 2214-2126. doi: https://doi.org/10.1016/j.jisa.2021.102771.
- Shivansh Kumar, Aman Kumar Bharti, and Ruhul Amin. **Decentralized secure storage of medical records using blockchain and ipfs: A comparative analysis with future directions. Security and Privacy,** 4(5):e162, 2021.
- Rosco Kalis and Adam Belloum. **Validating data integrity with blockchain.** In 2018 IEEE International Conference on Cloud Computing Technology and Science (CloudCom), pages 272–277, 2018. doi: 10.1109/CloudCom2018.2018.00060.
- Nishara Nizamuddin and Ahed Abugabah. Blockchain for automotive: **An insight towards the ipfs blockchain-based auto insurance sector.** International Journal of Electrical & Computer Engineering (2088-8708), 11(3), 2021.
- Ammar Ayman Battah, Mohammad Moussa Madine, Hamad Alzaabi, Ibrar Yaqoob, Khaled Salah, and Raja Jayaraman. **Blockchain-based multi-party authorization for accessing ipfs encrypted data.** IEEE Access, 8:196813–196825, 2020. doi: 10.1109/ACCESS.2020.3034260.

SOLUTION PROJECT

https://github.com/asahicantu/NFT-Thesis