2022 IEEE International Conference on Cloud Computing Technology and Science (CloudCom) | 978-1-6654-6367-6/22/$31.00 ©2022 IEEE | DOI: 10.1109/CloudCom55334.2022.00024

NFT as a proof of Digital Ownership-reward system integrated to a Secure Distributed Computing Blockchain Framework

Asahi Cantu
University of Stavanger
Stavanger, Norway
asahicantu@outlook.com

Jiahui Geng
University of Stavanger
Stavanger, Norway
jiahui.geng@uis.no

Chunming Rong
University of Stavanger
Stavanger, Norway
chunming.rong@uis.no

***Abstract*—Today, the global economy is dependent on the Internet and computational resources. Although they are tightly interconnected, it is difficult to evaluate their degree of interdependence. Keeping up with the pace of technology can be a challenging task, mainly when updating the hardware and software infrastructure. Every day, corporations and governments are faced with this issue; most have been victims of cyber attacks, security breaches, and data leaks. The consequences are significant in monetary losses; damage remediation is unattainable, even impossible, in certain circumstances. The repercussions might include reputational damage, legal responsibility, and threats to national security (when attacks are carried out against critical infrastructures to control the resources of a country), to name a few. Similarly, data has become such an integral part of many industries that it is one of the most critical targets for attackers that often is encrypted by ransomware, stolen, or corrupted. Without data, many companies are not able to continue operating as they do. The combination of all these factors complicates the ability of organizations to cooperate, trust, and share information in efforts to research and develop solutions for industry and government.**

This work proposes a Blockchain-based infrastructure solution provided by "Hyperledger Fabric" technology for companies to securely transmit and share information using the latest encryption and data storage technologies operating on the model of distributed systems and smart contracts. By presenting unique digital assets as Non-Fungible Tokens (NFT), the infrastructure is able to trust the integrity of the data, while protecting it from counterfeiting. Through the use of a Blockchain-based file storage system known as IPFS, and by connecting all the relevant elements together through a web-based application, it is possible to demonstrate that the implementation of such systems is feasible, highly scalable and a useful tool that many organizations can utilize to create new work systems and workflows for digital asset management.

***Index Terms*—blockchain, Hyperledger Fabric, NFT, IPFS, Digital Ownership**

I. Introduction

A promising technology can assist in significantly reducing the damage caused by the security threats outlined above: Blockchain technology has proven to be one of the most promising inventions of the twenty-first century for transmitting and protecting information while offering high reliability and availability, low exposure to attacks, protected encrypted data, and accessiblility to the entities willing to participate. Blockchain makes immutable data and compilability possible. The source code is called a "smart contract" where certain rules can be used to create business workflows.

As Blockchain technologies attract the interest of worldwide industries for their intrinsic values, new possibilities unleash to promote mutual cooperation in benefit of building up and improving technologies securely and manageable [11]. Companies can benefit from such systems when through inter-organizational trust, privacy and protection, improving and protecting businesses while cooperating and sharing information through a common system. When it comes to large-volume data sharing and storage, it becomes vital to verify its authenticity and avoid plagiarism/counterfeiting. The project proposes a system for the treatment of data as a digital asset through the concept of smart contracts [18] to manage Non-fungibility in a Blockchain system, and a server/application infrastructure to expose the potential and possibilities that data ownership can have when it is brought into decentralized permissioned systems with Hyperledger Fabric as a Blockchain system and Interplanetary File System (IPFS) as a Distributed File System (DFS) system.

The digital era keeps evolving and cloud computing increases its power. Users and companies are no longer in full control of their resources, rather than that, they led third party companies to store their information without fully knowing the way or locations it could be. In addition to this, recent cyber security risks and the progress of malware, ransomware and other harmful technologies have put the whole world into a cyber crisis. Ever since the creation of the interned such cyber attacks have been increasing exponentially and represent risks for the assets of the companies, countries and end users. Data keeps breaching and leaking sometimes without event noticing but months after the damage has happened.

This brings the need for an implementation of a more secure way to store and manage data through the internet without suffering from the present security risks.

Decentralized systems and Blockchain technologies created in the last ten years offer a tremendous potential to bring

978-1-6654-6367-6/22/$31.00 ©2022 IEEE
DOI 10.1109/CloudCom55334.2022.00024

organizations into a new way to manage their virtual assets.

It is therefore the purpose of this project to create an architecture and functional system to record unique ownership of digital assets in a permissioned blockchain (datasets ownership) while providing the infrastructure to allow its usage or deny it depending on the agreements of the system through the issuance of NFT's and smart contracts as an alternative solution that allows to alleviate the present cyber security risks while enabling data management securely and privately.

II. Background

Ever since the world has been interconnected over the Internet, malicious parties have intended to take advantage of their computational resources and digital assets. As technologies improve and the society evolves into a digital world, attacks become more sophisticated, frequent and devastating. It is increasing month by month in an exponential ways, compromising governments' and companies' systems and data.

Such has been the risk and consequences of cyber attacks and data breaches that in 2021 [19]:

1) On average a data breach costs up to 8.64 million USD.
2) Global Cybercrime costed over 6 trillion.
3) Businesses fell victim of ransomware every 11 seconds.
4) Took up to 220 days to contain a data breach, with healthcare industry being the slowest to recover with over 320 days.
5) As more users perform remote works cybercriminals keep increasing their attacks over telecommuters and remote access pathways.
6) Properly containing a data breach could have saved up to 1 million USD in less than 200 days
7) More than 8 TB of data were leaked.
8) A total of 270 major data breaches occurred, exposing 238 Million of records and 16 billion USD per day.

Moreover, in 2021 several Nordic companies were victim of important cyber attacks, peaking in December 2021 [14]. Affected industries include the largest industrial, food and service-providing sectors in the region.

III. Related work

1) e-Health: Healthcare systems maintain electronic medical records using the centralized storage models, potentially compromising user privacy. Potential threats include unauthorized access to critical information such as identity details, diseases from which a patient suffers, and misuse of patients' data. IPFS and blockchain technology, a distributed off-chain storage of medical data, can be created while preserving patient privacy.

- Kumar et al. [9] proposes a framework to facilitate easy access to medical data by authorized entities while preserving consistency, integrity, and availability.
- Chen et al. [5] suggests a system able to handle electronic health systems. for diabetes disease detection that provides an earlier detection of this disease by using various machine learning classification algorithms and securing the information. Blockchain, and IPFS are used to collect patients' health information via wearable sensor devices.
- Kumar et al. [10] proposes in the same manner a decentralized system for medical data storage that allows the community to securely share information and remove it from central systems since the high cost of data breaches, cyber attacks and the implicit cost of restructuring the IT infrastructure would prevent the progress in medical research and creation of new medical alternatives.
- Vahak [7] is an interesting project aiming to provide a low-latency, secure and reliable infrastructure via Ethereum smart contracts, 5-G and IPFS to allow communication and navigation of UAVs and improve the air-distribution of medical supplies in areas hard to reach or in crisis.
- HealChain [12] is a decentralized DMS for Mobile Healthcare Using Consortium Blockchain, that aims to build a system where security prevails when patients share medical data wirelessly.

2) Patents and intellectual property:

- Bamakan et al. [2] intends to apply NFT-based patent framework in public Blockchain networks and divers DFS to the intellectual property to promote transparency and liquidity for innovators willing to commercialize their inventions or be funded.
- Agyekum et al. [1] propose a digital media copyright and content protection using IPFS and Blockchain to expedite traditional digital copyright solidification and rights which are time consuming and labor-intensive using Hyperledger Fabric and the management of digital fingerprints for patents, ensuring immutability and provenance.
- Belloum et al. [8] models a data Integrity and confidentiality framework using encryption, smart contracts and Apache Isis for the automatic audit trial.

3) Automotive: Nizamuddin et al. [13] proposes an IPFS/Ethereum blockchain-based system for the auto insurance sector to solve the problem of fraud and latency and bureaucracy that customers face whenever acquiring insurance for vehicles.

4) Identity and Authorization: Battah et al. [3] present a solution for Blockchain-based MPA for Accessing IPFS Encrypted Data using Ethereum smart contracts and proxy re-encryption algorithms. It incorporates reputation mechanisms in the smart contracts to rate the oracles based on their malicious and non-malicious behaviors. Thus, this system can solve insider's attack problem by ensuring that a single authority or party is not acting alone.

5) Tourism: Demirel et al. [6] have created a model with Blockchain and IPFS integration for post pandemic economy for the tourism industry to fill the gap in the existing methods related to the use of the IoT, devices with smart contracts without a need for intermediaries for the reservations and services secured by Blockchain. The authors have created a booking system with a unique smart contract between customers and

hotels, including all services that a customer may need and elimination commission fees as well as reception costs.

6) Agriculture: Salah et al. [16] have created a Blockchain-Based Soybean Traceability in Agricultural Supply Chain by utilizing smart contracts to govern and control all interactions and transactions among all the participants involved within the supply chain ecosystem. All transactions are recorded and stored in the ledger with links to IPFS and thus providing to all a high level of transparency and traceability into the supply chain ecosystem in a secure, trusted, reliable, and efficient manner.

IV. Proposed Approach

This work uses a Hyperledger Fabric permissioned Blockchain framework as a base platform to implement an ERC-721 smart contract extension for the creation and certification of digital assets. It also implements a distributed data lake infrastructure through the usage of a private IPFS network, which allows storage of information in a reliable and trustless manner. When this data is linked to the ERC-721 smart contract, an NFT asset is created, and single entity properties like ownership, authenticity, transfer, royalties, etc, can be exposed to all its participants. No matter how many parties or users join the infrastructure, the consensus mechanism will ensure that the principle of immutability remains consistent across the network.

This project demonstrates through the creation of a back-end and front-end example applications the potential of its usage through a simulated token minting and data sharing environment among different known parties where the unique source of trust is a central authority and the previous agreement of the rules (consensus protocol) through which the data can be generated, shared and transferred in the same manner as if a crypto asset was transferred. Since the environment has been implemented using Docker Containers Technology, its scalability and security are granted and can be easily implemented. The results can be visualized in the following github repository, the program can be downloaded and deployed on any computer system with specific requirements

- ERC-721 protocol creation and extension
- Consensus mechanism
- Infrastructure and Blockchain environment in Hyperledger Fabric
- REST API in the back-end for common collaboration with the blockchain
- Front new Web application as a simulation of work and data generation through the blockchain
- Creation of a private IPFS network and data persistence schema for common data sharing

V. Detailed Implementation

Having proposed the hypothesis to solve inter-organization data sharing and transmission through secure channels, the implementation of the system is shown in this section.

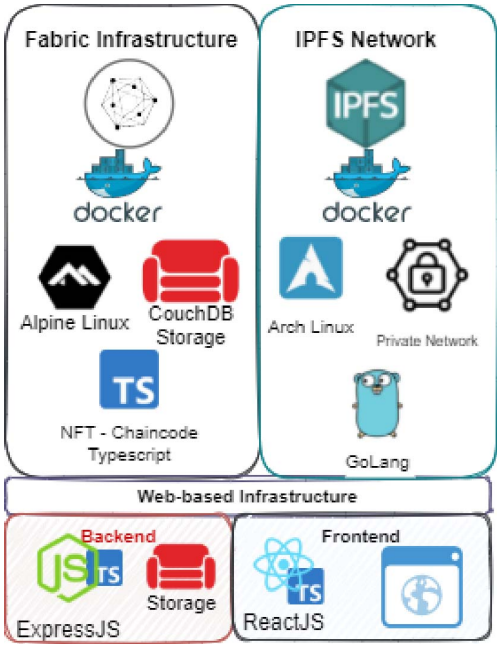

Fig. 1. Technologies used for the system implementation

1) System technologies: As demonstrated in Figure 1, our system uses the following technologies:

- **Docker**. Set of platform as a service products that use OS-level virtualization to deliver software in packages called containers.
- **Hyperledger Fabric** . Version 2.2 is used in the system. It uses Docker technology to run and simulate the system.
- **Typescript**. A programming language superset of JavaScript developed and maintained by Microsoft. This code was used to develop the chaincode, back-end and front-end systems.
- **ExpressJS**. Back-end web application framework for Node.js designed for building web applications and APIs.
- **React**. Open-source front-end JavaScript library for building user interfaces based on UI components.
- **Apache CouchDB**. NoSQL document-oriented open-source database.
- **IPFS** [4]. Decentralized file storage system used content-addressed capabilities configured as a private network.

2) Proposed architecture: The components are configured and assembled to integrate the infrastructure as in Figure 2

- **Hyperledger Fabric**. A a set of shell scripts and docker files assemble the required infrastructure to build the DLT. The Fabric infrastructure has the following subcomponents:
  1) Organizations. Two organizations have been created. One organization is built primarily to simulate the minting process of a NFT whereas the other can receive the minted token. The same process can also be made in the opposite way.

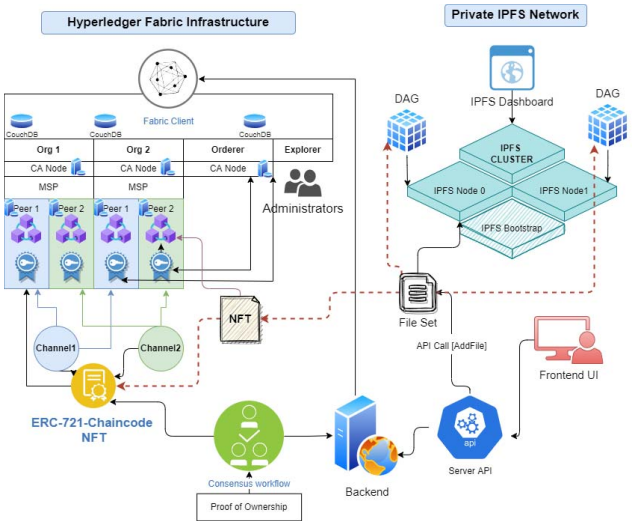

Fig. 2. Proposed Architecture

2) Orderer node. Is the node in charge of sorting the transaction and creating the block. Once the block is created, it is forwarded to one of the organizations holding the Blockchain ledger. The orderer node does not hold a copy of the ledger but just coordinates and distributes the issued transactions.
3) Orderer CA. Is the node in charge of issuing and validating the certificates of the organizations and the wallet creation (based on the root certificates) for the users to interact with the system.
4) Channel. Organizations in Hyperledger can join and interact through a private channel. The channel is previously known by the two organizations and they participate by having a server that holds a version of the ledger, a database server and a certificate authority server.
5) Chaincode. The smart contract used to manage the ledger transaction and mint digital assets as NFTs.

- **Private IPFS network**. It consists of a set of Docker containers where each system holds a copy of the IPFS file system [4].
  - IPFS bootstrap node. In the same way as the Ordered node receives the blocks of a transaction and transmits it to the organization nodes, it receives the file or data and transmits it to all the interconnected nodes, ensuring data persistence among the network.
  - IPFS Dashboard. It works as the UI of the private network. Provides insights and data about the stored files and a preview of the data once a user can access through its content.
  - IPFS Nodes. Each organization can contribute to the system data repository by holding an IPFS server.
- **Back-end**. Server application that communicates with the Hyperledger network and extends its functionality by an API.
  - Connects organizations and corporate databases
  - Communicates with the CA servers to issue and hold certificates.
  - Communicates with IPFS private network API.
  - Holds a public REST API that provides all the functionality to register organizations, enroll users and mint NFTs.
  - Interacts with the Blockchain smart contract and retrieves the information contained in the ledger.
- **Front-end**. It serves as the UI for user interaction. Allows the simulation of the system where any user can create an organization, enroll users, mint a NFT and visualize them in the list.

VI. Evaluation

To simulate the system functionality a case for two persons from different organizations trying to issue and mint data, send it and making it available to one another.

A. Setup and Scenario

In our scenario, two organizations need to share data with each other.

1) Organization 1: represents an organization with critical information gathered from external resources, expensive and difficult to obtain.

”Organization 1” creates a user **”Minter”** as a company representative in charge of submitting the data and creating a NFT version of it inside the system. Then he can use the system to lend the data, enable a time frame visualization or transfer it.

2) Organization 2: represents a technology company with skillful personal in data processing and domain area in the business of ”Organization 1”, but does not have the experience nor technology to gather it. Therefore it needs data from the organization mentioned above in order to create and expand their business.

”Organization 2” creates a user **”Receiver”** as a company representative in charge of getting access to the NFT minted data by ”Organization 1” via user ”Minter” which will be used as the data source to perform machine learning training operations.

With the NFT System framework, these parties can cooperate and participate by trusting that the information is secure, has not been altered, and can be easily verified by them and other parties.

VII. Results

The complete simulation of the process is shown in this section.

A. System registering and user enrollment

The NFT system provides a friendly user interface to allow organizations to be registered into the Fabric network to use a specific channel. Prior to this process Fabric generated a

CA with which they can identify as trusted entities and fair participants of the network.

The first time an organization registers itself to join a private channel, an admin account is created. The admin account then is able to configure organization parameters and new users with restricted access or different mining/system-usage capabilities. The process any organization will take to register itself as a valid participant with its corresponding representatives can be visualized in the figure 3 .

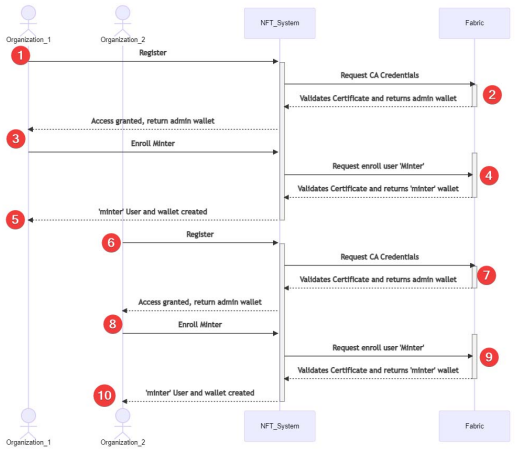

Fig. 3. Sequence diagram of the Organization and user enrollment process in the system.

B. NFT Minting and data reading access

Once the organizations and users have been properly enrolled, the following steps must occur:

1) Minter access to the platform and selects the ”Mint NFT option.
2) Minter selects a file and completes the form metadata.
3) Minter clocks on ”submit” button to create the token.
4) The system verifies that the file does not exist yet by:
   - Asking to add the data file to the IPFS network
   - Asking to Fabric if there is any token with the corresponding CID

   For any of those cases to be true, the token will not be generated and an error will be returned.
5) Once everything is approved, the token is stored in the DLT with the corresponding file CID generated.
6) ’Minter’ can now send the CID or additional token information to ’Receiver’. Then receiver can pull such information from the infrastructure. Because of its unicity purposes ’Receiver’ will not be able to counterfeit or take ownership of the data unless explicitly stipulated and agreed by both parties.

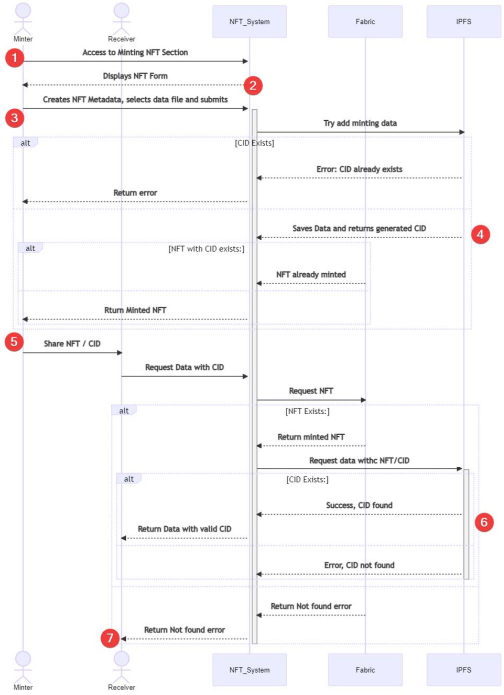

Fig. 4. Sequence diagram to mint a NFT

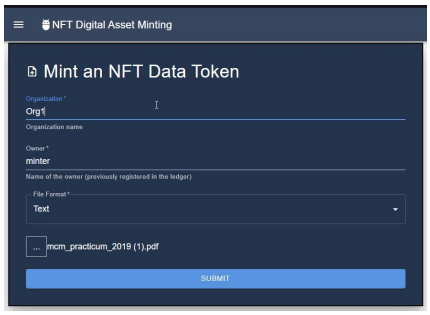

Fig. 5. Front-end showing minting process.

C. NFT Transfer

It is possible through the REST API to transfer the generated tokens from one owner to the other. This process will acknowledge that the new user is the new owner of the NFT. It is possible then to track the chain of ownership.

D. NFT Burning

The system also supports burning an NFT, which basically blocks the token and flags it as unusable. if that happens, burned NFT and CID data cannot be accessed via the platform.

IT is possible, however to access the data via the IPFS server.

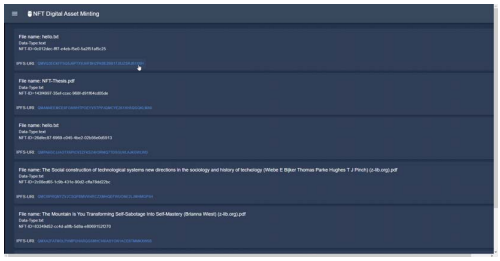

Fig. 6. Front-end showing minted NFTs in the system.

VIII. Discussion

The implementation of digital asset management through issuance of NFTs represents a milestone in the generation of decentralized secure frameworks for industrial applications.

The implicit security of Blockchain with Hyperledger management and the privacy such technology offers will allow different organizations to participate and cooperate securely, but not anonymously.

All parties will be able to acknowledge data ownership. If desired, data could be encrypted as well and managed through additional smart contracts. In addition to this, IPFS network is able to control, distribute and manage the added data as a DFS. The final simulation of the environment allows testers, to acknowledge the workflow of the framework and further expand its capabilities in a modular way.

IX. Results

The simulation was performed with the following operations:

1) Minting NFT with Text data 10KB
2) Minting NFT with Image data 200KB
3) Minting NFT with Bin data 100MB
4) Minting NFT with a file of 850MB

The highest resource consuming process for the system is whenever data with high space resources are about to be minted. The communication with the server and IPFS network create a bottleneck in the simulation process and by running the resources locally.

NFT Statistics			
No	File type	Size	Elapsed time (s)
1	Text	10KB	0.5
2	Image	200KB	1.3
3	PDF	100MB	8.3
4	Bin	850MB	∞

TABLE I
NFT Statistics.

Whenever trying to mint an NFT File larger than 500 MB (previous tests were made with other files) the blockchain system, or at least the API server takes significantly larger amount of time than expected to submit the data. Although this might be a parameter or server side configuration, it certainly refrains users from submitting large amounts of information.

Final results of the built application indicate that it is potentially feasible to create decentralized systems specialized in data management and control for industrial purposes while dealing with chunks of data. For text data it is relatively easy to mint, submit and visualize under the IPFS Server.

A. Infrastructure statistics

The following statistics were performed by running *docker stats* command where they where later on plotted.

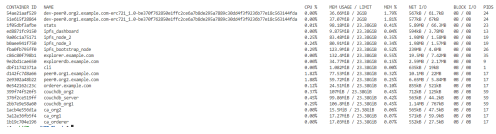

Fig. 7. Docker statistics from current containers

B. Benchmarking and Blockchain metrics evaluation

Hyperledger framework has a benchmark tool used to measure the performance and behavior of the blockchain, test it and evaluate it under stress scenarios to check its latency and behaviour under heavy usage. Tables II and III show the results thrown in raw data. Figure 8 presents relevant information about the usage and network stress results. as an HTML report, which is also available at: https://htmlpreview.github.io/?https://raw.githubusercontent.com/asahicantu/NFT-Thesis/main/caliper-benchmarks/report.html Units of measure for the data are in s and TPS.

Blockchain benchmark Part I.				
Name	Succ	Fail	Send Rate (TPS)	Max Latency(s)
MintNFT.	5000	0	15.0	2.19
Query all NFTS.	9819	0	338.2	0.06

TABLE II
Blockchain Benchmark using Hyperledger Caliper Part I.

Blockchain Benchmark using Hyperledger Caliper Part II.			
Name	Min Latency (s)	Avg Latency (s)	Throughput (TPS)
MintNFT.	0.10	0.43	14.9
Query all NFTS.	0.01	0.02	338.1

TABLE III
Blockchain Benchmark using Hyperledger Caliper Part II.

X. Conclusions

In line with the original hypothesis it is possible to confirm that the construction of decentralized systems is possible and will create yet unforeseen possibilities to manage information and provide:

- System scalability
- Modularity
- Self Governance by smart contract agreement
- Privacy and security

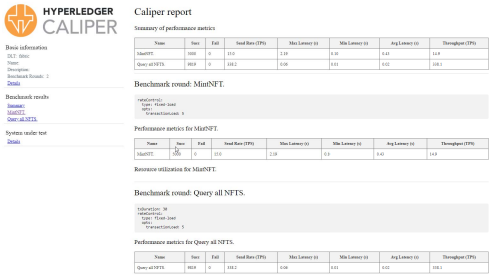

Fig. 8. Hyperledger Caliper Benchmark results.

- Mutual cooperation

Systems such as this can be governed or not by a central authority. Depending on the business needs and industrial purposes different scenarios could be developed and simulated.

Key findings through the research and development of this project are:

A. Blockchain and DLT

Data integrity and consistency safeguarding. Decentralized system nowadays allow very easily to verify data origin, integrity and non-repudation principle establishes new ways of working and contributing for the development and research of technology.

B. Security

The created infrastructure has several layers of security and implicit elements to protect parties and their data from improperly accessing information.

1) CAs: Different parties can choose to rely over a central or multiple CAs. As long as there is a common agreement previously established by smart contracts and common consensus, it will be possible to create highly resistant and resilient systems to malicious attacks. The modularity of Blockchain allows the cooperation of parties to benefit the whole system, therefore rejecting undesirable or suspicious behaviour.

2) Private channels: Private channels in Hyperledger Fabric allow organizations to create a subsystem inside the framework, where sub smart contracts can be created to allow privacy between a single, two or more entities in different regions of the world. Therefore, while every organization can hold a copy of the ledger and data, only those with the right privileges can be allowed to interact with the hidden rules.

IPFS offers several layers of security, data can be encrypted and directed by smart contract instructions and even by the security layers set into the built system.

C. Governance

Organizations can self in their best interest to preserve business functionality and choose the most suitable way to manage data. That being said, they will be able to choose which CA is the best, and what rules in the smart contract can be implemented and under which conditions entities can mint or transfer NFTs.

XI. Future Work

It is intended for anyone willing to extend and expand the functionality of this work to move within the following points:

A. System integration

This project can complement the work made by [15], which explains how shared data can be used to perform workflows for different purposes such as Big data analytics and Machine learning. One key advantage of this implementation relies on the fact that participants will have no direct access to shared data itself, but to a framework where it can be processed and manipulated to generate different models and insights. When connecting both systems, it will be possible to create and encapsulate information. Data encryption can grant that even different organizations own a copy of the blockchain and IPFS network, they cannot read the information unless they do it directly from the proposed application.

B. NFT and Smart Contract extension

An extension of ERC-721 [17] smart contract implemented can be easily extended to create new business rules such as:

1) NFT delegated ownership and transfer: Not only one user, but multiple entities could possess a digital asset, sharing a percentage of such element. Therefore new rules can be suggested to interact, protect and manipulate information.

2) Consensus: New consensus mechanisms can be generated to incentivize the usage of the network. This project contains for example rules to rank information and create a reputation level for the organizations, which can increase the value of the minted NFT. In other scenarios can be possible to create digital ownership by data origin, geographical location and mechanisms of burning so it cannot be used by other parties.

3) Economics through Tokenization: A very interesting approach to explore is the creation of economic tokens integrated with the NFT system. Such tokens and in the same form that ETH does with the Ethereum platform, every piece of data can be linked to another unity of tokens where once transferred its value in tokens can be transferred as well. The token-value of data can increase as its ranking of ”valuable information” increases, or organization’s reputation does. Depending on those economic mechanisms, different companies could be able to generate royalties and incentivize the usage of the system. Furthermore.

4) Multi-system integration: Furthermore, this project can be integrated with other public Blockchain platforms, and allow the issuance or reading of Ethereum smart contracts, enabling its execution in the internal network. The possibilities are endless and adaptable to specific business needs.

References

[1] Kwame Opuni-Boachie Obour Agyekum, Qi Xia, Yansong Liu, Hong Pu, Christian Nii Aflah Cobblah, Goodlet Akwasi Kusi, Hanlin Yang, and Jianbin Gao. Digital media copyright and content protection using ipfs and blockchain. In *International Conference on Image and Graphics*, pages 266–277. Springer, 2019.

[2] Seyed Mojtaba Hosseini Bamakan, Nasim Nezhadsistani, Omid Bodaghi, and Qiang Qu. Patents and intellectual property assets as non-fungible tokens; key technologies and challenges. *Scientific Reports*, 12(1):1–13, 2022.

[3] 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.

[4] Juan Benet. Ipfs-content addressed, versioned, p2p file system. https://ipfs.io/ipfs/QmR7GSQM93Cx5eAg6a6yRzNde1FQv7uL6X1o4k7zrJa3LX/ipfs.draft3.pdf, 2014.

[5] 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.

[6] Engin Demirel, Seda Karagöz Zeren, and Kemal Hakan. Smart contracts in tourism industry: a model with blockchain integration for post pandemic economy. *Current Issues in Tourism*, pages 1–15, 2021.

[7] Rajesh Gupta, Arpit Shukla, Parimal Mehta, Pronaya Bhattacharya, Sudeep Tanwar, Sudhanshu Tyagi, and Neeraj Kumar. Vahak: A blockchain-based outdoor delivery scheme using uav for healthcare 4.0 services. In *IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pages 255–260, 2020.

[8] 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.

[9] Randhir Kumar, Ningrinla Marchang, and Rakesh Tripathi. Distributed off-chain storage of patient diagnostic reports in healthcare system using ipfs and blockchain. In *2020 International Conference on COMmunication Systems NETworkS (COMSNETS)*, pages 1–5, 2020.

[10] 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.

[11] Satoshi Nakamoto. Bitcoin whitepaper. *URL: https://bitcoin. org/bitcoin. pdf-(: 17.07. 2019)*, 2008.

[12] Weiquan Ni, Xumin Huang, Junxing Zhang, and Rong Yu. Healchain: A decentralized data management system for mobile healthcare using consortium blockchain. In *2019 Chinese Control Conference (CCC)*, pages 6333–6338, 2019.

[13] 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.

[14] Gerard O'Dwye. Nordic companies targeted in wave of cyber attacks. https://www.computerweekly.com/news/252511965/Nordic-companies-targeted-in-wave-of-cyber-attacks, 01 2022. (Accessed on 05/16/2022).

[15] Ali Akbar Rehman. System for workflow design and execution on data shared between untrusting organizations for analytics. Master's thesis, University of Stavanger, Norway, 6 2022.

[16] Khaled Salah, Nishara Nizamuddin, Raja Jayaraman, and Mohammad Omar. Blockchain-based soybean traceability in agricultural supply chain. *IEEE Access*, 7:73295–73305, 2019.

[17] superphiz. Erc-721 non-fungible token standard — ethereum.org. https://ethereum.org/en/developers/docs/standards/tokens/erc-721/. (Accessed on 06/14/2022).

[18] Ethereum Foundation Vitalik Buterin. Erc — ethereum improvement proposals. https://eips.ethereum.org/erc, 2019. (Accessed on 05/14/2022).

[19] Wickr. 10 data breach statistics for 2021 - wickr. https://wickr.com/10-data-breach-statistics-for-2021/, 2021. (Accessed on 05/16/2022).