IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, June 2023

Decentralized Attestation and Distribution of Information using Blockchains and Multi-Protocol Storage

Prof. Rahul Raut, Nilesh Aher, Yogeshkumar Jagtap, Vaibhav Jamdhade, Rutvik Kalamkar
Department of Information Technology
Sandip Institute of Technology and Research Centre, Nashik, India

Abstract: *If blockchain networks are to become the building blocks of the infrastructure for the future digital economy, then several challenges related to the resiliency and survivability of blockchain networks need to be addressed. The survivability of a blockchain network is influenced by the diversity of its nodes. Trustworthy device-level attestations permits nodes in a blockchain network to provide truthful evidence regarding their current configuration, operational state, keying material and other system attributes. In the current work we review the recent developments towards a standard attestation architecture and evidence conveyance protocols. We explore the applicability and benefits of a standard attestation architecture to blockchain networks. Finally, we discuss a number of open challenges related to node attestations that has arisen due to changing model of blockchain network deployments, such as the use virtualization and containerization technologies for nodes in cloud infrastructures.*

Keywords: Attestation, Ipfs, Decentralized Storage, etc

I. INTRODUCTION

We believe there is a crucial role for trusted computing technologies, and more specially attestations technologies, within the nascent area of blockchain networks. As blockchain networks play an increasing role in the future digital economy – such as becoming the underlying infrastructure for future crypto-currencies and virtual assets exchange networks – the security, resiliency and survivability of blockchain systems becomes crucial to their business value-proposition. Since the dawn of the computer age and the development of networked computer systems and the Internet, there has been the need for operators of computing equipment to obtain correct and truthful insights into the state of computing devices as part of managing the security of these devices. Given the proliferation of malware and viruses in the past decade, there has been a need for networked devices to have the capability to report its configuration, internal state and other parameters in a truthful and unforgeable manner. The technical term used to describe this process is attestations. The goal of the current work is threefold. The first is to review the current development towards a standard attestation architecture in the computer and network industry. Secondly, to explore the applicability and benefits of the attestations architecture to nodes in a blockchain network. Thirdly, we discuss some of the current challenges in attestations that has arisen due to changing model of blockchain networks, such as the use virtualization technologies for nodes in cloud infrastructures.

II. LITERATURE SURVEY

Decentralized attestation :-Author is F. Harer and H.-G.-Fill Decentralized attestation methods for blockchains are currently being discussed and standardized for use cases such as certification, identity and existence proofs. In a blockchain based attestation, a claim made about the existence of information can be cryptographically verified publicly and transparently.

Blockchain System-A blockchain is a data structure of linked blocks, where each block is linked to one predecessor by the value of a hash function for providing integrity across the chain.

Attestation Concept- In the context of conceptual modeling, these ideas can be applied for the remote attestation of model artifacts, bound to the identity of a user. Here, a model-based attestation can be conducted by (A.) the creation of

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, June 2023

a claim about the existence of a model, bound to an identity (B.) the validation of the claim by any other identity at a later point in time. In such a system, an attestation can be conducted by the issuance of a claim through a user, referred to as Claim Issuer, who records the claim for it to become part of the trusted global state, and by validating the claim through a user, referred to as Claim Validator.

Towards an attestation architecture for blockchain networks.The Author is Thomas Hardjono, Ned Smith
If blockchain networks are to become the building blocks of the infrastructure for the future digital economy, then several challenges related to the resiliency and survivability of blockchain networks need to be addressed. The survivability of a blockchain network is influenced by the diversity of its nodes. Trustworthy device-level attestations permits nodes in a blockchain network to provide truthful evidence regarding their current configuration, operational state, keying material and other system attributes. In the current work we review the recent developments towards a standard attestation architecture and evidence conveyance protocols. We explore the applicability and benefits of a standard attestation architecture to blockchain networks. Finally, we discuss a number of open challenges related to node attestations that has arisen due to changing model of blockchain network deployments, such as the use of virtualization and containerization technologies for nodes in cloud infrastructure.

Towards a decentralized process for scientific publication and peer review using blockchain and IPFS.The Author is A. Tenorio-Fornés, V. Jacynycz, D. Llop-Vila-In recent years, the increasing concerns around the centralized cloud web services (e.g. privacy, governance, surveillance, security) have triggered the emergence of new distributed technologies, such as IPFS or the Blockchain. These innovations have tackled technical challenges that were unresolved until their appearance. Existing models of peer-to-peer systems need a revision to cover the spectrum of potential systems that can be now implemented as peer-to-peer systems. This work presents a framework to build these systems. It uses an agent-oriented approach in an open environment where agents have only partial information of the system data. The proposal covers data access, data discovery and data trust in peer-to-peer systems where different actors may interact. The technological innovations that enable the development of new peer-to-peer systems previously unfeasible that this paper studies and some of its underlying concepts such as content-addressability and merkle linked structures. Content Addressability In centralized and federated systems, content is frequently referred with addresses that include location information, the Uniform Resource Locators (URLs). However, references to content can also be independent from their location, using Universal Resource Identifiers (URIs). In peer-to-peer systems, agents cannot rely on the location of other agents for accessing content, because the content could be provided by any agent. The hash1 of any content can be used as its URI. Thus, these hash URIs are used in multiple distributed systems such as IPFS to build scalable content-addressable networks. Merkle Links and Structures . This Merkle linked structures are key to build technologies such as Git, Blockchain and IPFS among others. Blockchain was the first technology that enabled a fully distributed digital currency. It uses a Merkle Linked list of blocks of transactions (a Blockchain) to build a distributed ledger of transactions. It made computationally difficult to propose a candidate for the next block in the distributed ledger and incentives nodes to try to build those candidates with valid transactions. Then, the protocol requires that honest nodes will consider the largest chain they have observed in a given time as the actual ledger to trust. Therefore, in order to forge a blockchain, an actor would need half of the computing power of the system. IPFS Some peer-to-peer systems like P2P sharing software use hash of the content to address it. Other technologies such as Git use complex Merkle-Linked Structures. IPFS integrates both the use of complex Merkle-Linked structure with the data-addressability of P2P file sharing systems. The content is distributed over a peer-to-peer network. Section proposes the use of IPFS for the storage and distribution of data in the framework.

Author: George Coker, Joshua Guttman, Peter Loscocco :-
Attestation is the activity of making a claim about properties of a target by supplying evidence to an appraiser. We identify five central principles to guide development of attestation systems. We argue that , (i) attestation must be able to deliver temporally fresh evidence; (ii) comprehensive information about the target should be accessible; (iii) the target, or its owner, should be able to constrain disclosure of information about the target; (iv) attestation claims should have explicit semantics to allow decisions to be derived from several claims; and (v) the underlying attestation

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, June 2023

mechanism must be trustworthy. We propose an architecture for attestation guided by these principles, as well as an implementation that adheres to this architecture. Virtualized platforms, which are increasingly well supported on stock hardware, provide a natural basis for our attestation architecture.

2.1 Problem Statement

As of today, data integrity of references is not verified and preserved, allowing for changes against the intention of the original source. As an example, consider a hyperlink from a website to a scientific dataset used for machine learning. If the referenced dataset changes, e.g. due to an update, the IRI may stay the same. Thus, any agent retrieving the dataset could not infer the integrity of the dataset just from thereference but would have to employ additional measures,e.g. as done today via checksums or digital signatures of theunderlying content . The original intention of the creator of the link may thus be violated without actually knowingabout the violation. Secondly, the availability of data cannot be guaranteed in traditional web architectures. Rather, one needs to trust the operators of the servers to continuously guarantee the availability of resources. In case data becomes unavailable, e.g. servers ceasing operation, the established web protocols do not support mechanisms to make data available again, even if it were present somewhere else in the network. With resources already available over protocols such as HTTP, it remains challenging to provide the properties of integrity and availability in a decentralized setting. This limits the long-term preservation of information and the traceability of information resources. Consider here as an example the need to access particular datasets for conducting research or for enabling machines toautomatically find and use data on request. Furthermore, the exact time of the issuance of information can today not be verified for arbitrary web resources. This is, however, necessary for scenarios where the time of issuance is of primary importance, e.g. for resolving disputes on intellectual property such as patents and trademarks without having to rely on a trusted third party such as a patent office.

2.2 Objectives

- To provide the attestation and distribution to the information by using blockchain technology and Multi-Protocol Storage.
- In combination with distributed ledgers, these applications can be realized based on the properties of integrity-secured and non-repudiable transactions bound to identities of users.
- To decentralized registries for documents, records or digital rights shared among organizations.

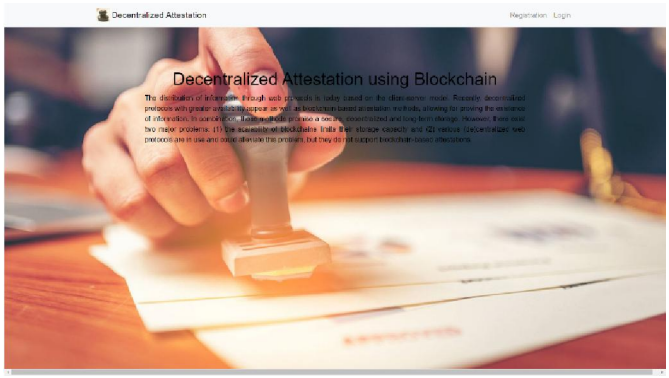
2.3 Proposed System

System Structure:- For achieving modularity, the system has been designed in the form of several components for carrying out attestations. First, a Claim Issuer (CI) initiates the distribution of files and the issuance of claims. Then, a Claim Validator(CV) retrieves files and validates corresponding attestations. No trusted relationship between CI and CV is assumed. Furthermore, CI, CV, or any untrusted third party are assumed to engage in the creation of links. The following assumptions are made for the components of the architecture: Corresponding to the architecture requirement of supporting multiple protocols, (1) a storage network is assumed where an arbitrary number of nodes provide services through web protocols, encompassing state-of-theart centralized and decentralized protocols. Nodes are assumed to be distributed, independent from each other, and reachable over private or public wide area networks. Related to the attestation, (2) a blockchain platform supporting smart contracts is assumed where an attestation smart contract can be deployed, e.g. on Ethereum. Due to the properties of blockchains, the autonomous execution of the smart contract is outside the control of CI, CV, and third parties. The functions of the smart contract will be discussed in detail in the following sections. (3) The URI scheme and link format and a client-side implementation required for automated validation are finally assumed. For validation purposes, a prototype implementation of the client realized the attested multi-protocol link immutability system (amplius).2 It supports the functions outlined in the following sections. The coordination of an attestation is managed in a decentralized fashion by the client in combination with the smart contract.

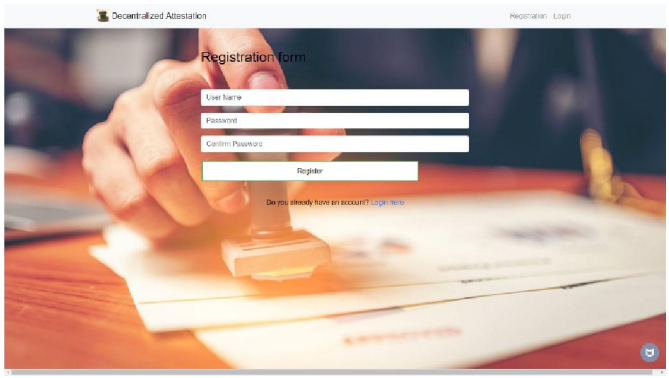
Distribution of Files in The Storage Network:- Initially, a file set F is locally available at the claim issuer CI. F contains any number of files for distribution through the storage network of a set of individual nodes N. For distribution and attestation on a per-file basis, F might contain only one element. Each client-initiated transfer operation involving files

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, June 2023

Fv⊆ F and node n ∈ N is represented by the function distribute :Fv, n → (Scheme, Authority, Path) which yields a tuple representing a single URI. The set of all URI tuples is denoted as URI_Set. No restrictions are imposed besides URI-based addressing. However, protocols might impose additional restrictions such as addressing F under a single repository URI, e.g. when using Git. There is no requirement for content-based storage on the protocol level. 3) Issuance And Recording Of Claims An attestation consists of a claim issued by claim issuer CI and the validation performed by claim validator CV. Thereby, a claim documents (1) the existence of F, (2) the possession of f by CI, and (3) the time of recording the claim Timestamp

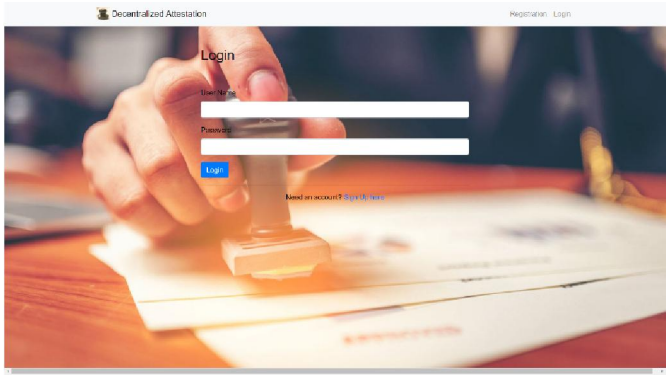


1. Landing Page Of Project



2. Registration Page

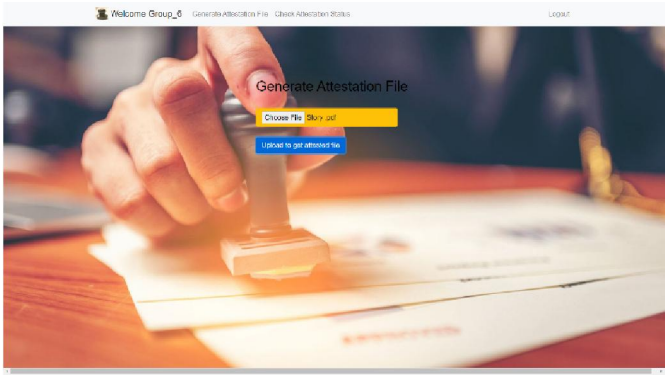
Registration Page - Page for new users to sign up for the service using their email address



3. Login Page

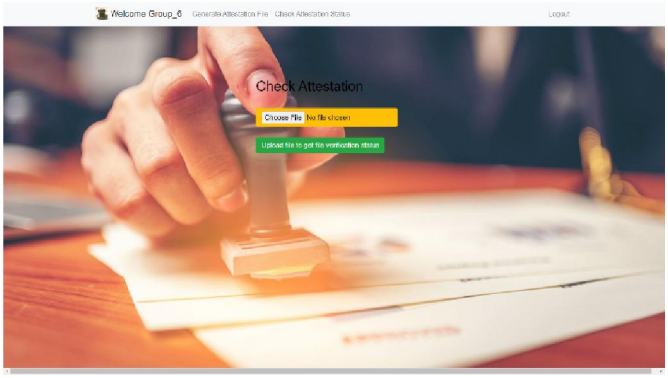
Login Page - Login page for users to login. Users must register before logging in

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, June 2023



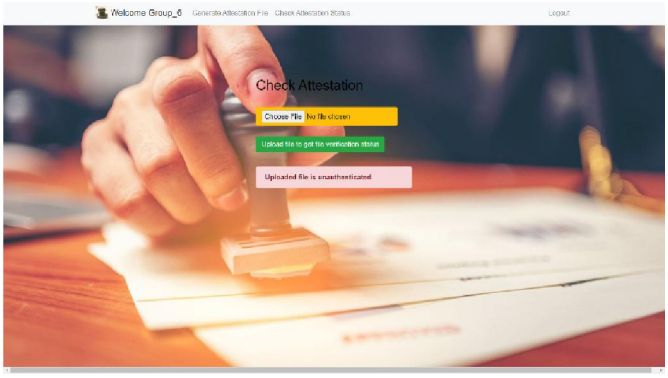
4. Generate Attestation File

Generate Attestation File -Interface to generate attestation via uploading the desired file.



5.Check Attestation File

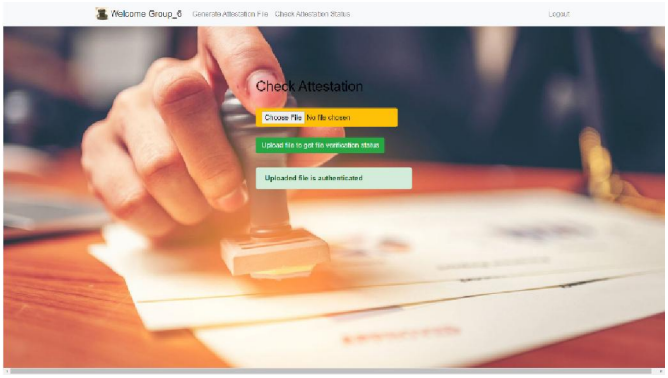
Check Attestation File - Interface to check valid attestation for previously attested file.



5.1Unauthorized File

Unauthorized File - Interface to show user that the attestation verification for the desired file is unauthorized. Some changes may have happened to original file

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, June 2023



5.2Authorized File

Authorized File- Interface to show user that the attestation verification for desired file is authorized. No changes occured in the file.

Hardware/Software Required Specifications

Hardware Requirements :

- **Processor:** 1 gigahertz (GHz) or faster processor
- **RAM:** 4 gigabytes (GB) for 32-bit or 8 GB for 64-bit
- **Hard disk space:** 512 GB for 32-bit OS or 1 TB for 64-bit OS

Software Requirements :

- Operating System: Ubuntu 14.0.4/Windows 10 RAM : 8GB
- Python version 3.9+
- Git
- IPFS
- Beautiful Soup

Outcomes

- At the end of the project Decentralised attestation responsible for the measurement of the data correctness , data authenticity and timestamp of the information.
- This method of information storage distribution promise a secure, decentralized and long term storage.

VI. CONCLUSION

In contrast to previous approaches, it reverts to a multi-protocol concept, which permits to augment existing storage protocols such as Git or IPFS with blockchain-based attestations for verifying the authenticity and timestamps of the stored information. Through a first prototypical implementation the technical feasibility of the approach could be positively evaluated. Further, measurements of the performance of the approach showed a constant size of transactions for recording links and a moderate cost and completion time when reverting to the public Ethereum blockchain. Future research will include in particular the extension of the approach towards other blockchain platforms. With the currently witnessed steep technological progress of blockchain platforms, it will be of interest to further study how higher transaction speeds and lower transaction costs will affect a more widespread adoption of the proposed approach. Similarly, the approach could be joined with blockchain-based mechanisms for processing the stored data, e.g. for reasoning over the content of data in a decentralized fashion to verify content-related properties.

VII. FUTURE SCOPE

A promising area addressing the limitations of availability and integrity are decentralized architectures using blockchains.

Inter-Planetary-File-System (IPFS) provides availability and resilience by replicating data across nodes of a network.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, June 2023

REFERENCES

[1] FELIX HÄRER AND HANS-GEORG FILL, "Distribution of Information Using Blockchains and Multi-Protocol Storage", (2022)
[2] Thomas Hardjono1 and Ned Smith, "An Attestation Architecture for Blockchain Networks", (2020)
[3] Digitalization and Information Systems Group, "Decentralized Attestation of Conceptual Models Using the Ethereum Blockchain", (2019)
[4] Antonio Tenorio-Fornés - Samer Hassan - Juan Pavón,"Thomas Hardjono1 ·Ned Smith, "Towards an attestation architecture for blockchain networks", (2021)
[5] Open Peer-to-Peer Systems over Blockchain and IPFS: an Agent Oriented Framework", (2018)
[6] George Coker, Joshua Guttman, Peter Loscocco, Justin Sheehy, and Brian Sniffen," Attestation: Evidence and Trust", (2018)
[7] Hans-Georg Fill , Felix Härer, "Storing and Attesting Conceptual Models on Blockchains", (2020)
[8]T.Hardjono,"BlockchainInteroperability and Survivability," September 2018, presentation 2018 IEEE Global Blockchain Summit, NIST, Gaithersburg, MD (17-19 September 2018).
[9] R. Hasan, Z. Anwar, W. Yurcik, L. Brumbaugh, and R. Campbell, ''A survey of peer-to-peer storage techniques for distributed file systems,'' in Proc. Int. Conf. Inf. Technol., Coding Comput. (ITCC), vol. 2, Apr. 2005.
[10]V. Buterin, G. Wood, and J. Wilcke. (2014). A Next-Generation Smart Contract and Decentralized Application Platform. Accessed: Nov. 26, 2021
[11]H. Huang, J. Lin, B. Zheng, Z. Zheng, and J. Bian, ''When blockchain meets distributed file systems: An overview, challenges, and open issues,'' IEEE Access, vol. 8, pp. 50574–50586, 2020
[12]G. Wood. (2014). Ethereum: A Secure Decentralised Generalised Transaction Ledger. Accessed: Feb. 8, 2019