**LITERATURE SURVEY**

1. **ProvChain: A Blockchain-Based Data Provenance Architecture in Cloud Environment with Enhanced Privacy and Availability**

**AUTHORS:**  X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat, and

L. Njilla

Cloud data provenance is metadata that records the history of the creation and operations performed on a cloud data object. Secure data provenance is crucial for data accountability, forensics and privacy. In this paper, we propose a decentralized and trusted cloud data provenance architecture using blockchain technology. Blockchain-based data provenance can provide tamper-proof records, enable the transparency of data accountability in the cloud, and help to enhance the privacy and availability of the provenance data. We make use of the cloud storage scenario and choose the cloud file as a data unit to detect user operations for collecting provenance data. We design and implement ProvChain, an architecture to collect and verify cloud data provenance, by embedding the provenance data into blockchain transactions. ProvChain operates mainly in three phases: (1) provenance data collection, (2) provenance data storage, and (3) provenance data validation. Results from performance evaluation demonstrate that ProvChain provides security features including tamper-proof provenance, user privacy and reliability with low overhead for the cloud storage applications.

1. **Towards Blockchain Tactics: Building Hybrid Decentralized Software Architectures**

**AUTHORS:** F. Wessling, C. Ehmke, O. Meyer, and V. Gruhn

Blockchain-based applications usually consist of centralized elements (e.g., web servers and back-end logic) connected to decentralized elements such as smart contracts. The engineering of such hybrid software architectures poses a challenge as it is unclear which elements should be centralized or decentralized. Furthermore the impact of this decision (or the balance between those two areas) on software quality attributes such as security, maintainability, performance or costs is currently unknown. The goal is to build a software architecture using the benefits and handling the challenges of blockchain technology while fulfilling the relevant quality attributes. While there are several approaches examining the relation between architectural decisions and quality attributes in centralized systems, research is at an early stage for decentralized elements in software architectures. This paper presents a first step towards architectural blockchain tactics. With a simplified experiment comparing two implementation variants of an Ethereum smart contract we show that software design patterns are not always beneficial and that the expected usage scenarios have a strong impact on the operational costs. We argue that further research and validation is necessary for gaining more qualitative and quantitative insights to make informed architectural design decisions when using blockchain technology and give a first outline on how to achieve this.

1. **Blockchain: A panacea for healthcare cloud-based data security and**

**privacy**

**AUTHORS:** C. Esposito, A. De Santis, G. Tortora, H. Chang, and K. R. Choo,

One particular trend observed in healthcare is the progressive shift of data and services to the cloud, partly due to convenience (e.g. availability of complete patient medical history in real-time) and savings (e.g. economics of healthcare data management). There are, however, limitations to using conventional cryptographic primitives and access control models to address security and privacy concerns in an increasingly cloud-based environment. In this paper, we study the potential to use the Blockchain technology to protect healthcare data hosted within the cloud. We also describe the practical challenges of such a proposition and further research that is required.

1. **Blockchain for AI: Review and Open Research Challenges**

**Authors: Khaled Salah; M. Habib Ur Rehman; Nishara Nizamuddin; Ala Al-Fuqaha**

Recently, artificial intelligence (AI) and blockchain have become two of the most trending and disruptive technologies. Blockchain technology has the ability to automate payment in cryptocurrency and to provide access to a shared ledger of data, transactions, and logs in a decentralized, secure, and trusted manner. Also with smart contracts, blockchain has the ability to govern interactions among participants with no intermediary or a trusted third party. AI, on the other hand, offers intelligence and decision-making capabilities for machines similar to humans. In this paper, we present a detailed survey on blockchain applications for AI. We review the literature, tabulate, and summarize the emerging blockchain applications, platforms, and protocols specifically targeting AI area. We also identify and discuss open research challenges of utilizing blockchain technologies for AI.

1. **Performance benchmarking and optimizing hyperledger fabric blockchain platform**

**AUTHORS: Parth Thakkar; Senthil Nathan; Balaji Viswanathan**

The rise in popularity of permissioned blockchain platforms in recent time is significant. Hyperledger Fabric is one such permissioned blockchain platform and one of the Hyperledger projects hosted by the Linux Foundation. The Fabric comprises various components such as smart-contracts, endorsers, committers, validators, and orderers. As the performance of blockchain platform is a major concern for enterprise applications, in this work, we perform a comprehensive empirical study to characterize the performance of Hyperledger Fabric and identify potential performance bottlenecks to gain a better understanding of the system. We follow a two-phased approach. In the first phase, our goal is to understand the impact of various configuration parameters such as block size, endorsement policy, channels, resource allocation, state database choice on the transaction throughput & latency to provide various guidelines on configuring these parameters. In addition, we also aim to identify performance bottlenecks and hotspots. We observed that (1) endorsement policy verification, (2) sequential policy validation of transactions in a block, and (3) state validation and commit (with CouchDB) were the three major bottlenecks. In the second phase, we focus on optimizing Hyperledger Fabric v1.0 based on our observations. We introduced and studied various simple optimizations such as aggressive caching for endorsement policy verification in the cryptography component (3x improvement in the performance) and parallelizing endorsement policy verification (7x improvement). Further, we enhanced and measured the effect of an existing bulk read/write optimization for CouchDB during state validation & commit phase (2.5x improvement). By combining all three optimizations1, we improved the overall throughput by 16x (i.e., from 140 tps to 2250 tps).