Chapter 5
Cloud-Centric Blockchain Public Key Infrastructure for Big Data Applications

Brian Tuan Khieu
San Jose State University, USA

Melody Moh
https://orcid.org/0000-0002-8313-6645
San Jose State University, USA

ABSTRACT

A cloud-based public key infrastructure (PKI) utilizing blockchain technology is proposed. Big data ecosystems have scalable and resilient needs that current PKI cannot satisfy. Enhancements include using blockchains to establish persistent access to certificate data and certificate revocation lists, decoupling of data from certificate authority, and hosting it on a cloud provider to tap into its traffic security measures. Instead of holding data within the transaction data fields, certificate data and status were embedded into smart contracts. The tests revealed a significant performance increase over that of both traditional and the version that stored data within blocks. The proposed method reduced the mining data size, and lowered the mining time to 6.6% of the time used for the block data storage method. Also, the mining gas cost per certificate was consequently cut by 87%. In summary, completely decoupling the certificate authority portion of a PKI and storing certificate data inside smart contracts yields a sizable performance boost while decreasing the attack surface.

INTRODUCTION

Verification of one's identity continues to be the cornerstone upon which any interactions or transactions between two parties lie. One key method of verifying one's identity is through using public and private keys, which are cryptographically related strings that can be used to lock and unlock files. If a public key is used to lock a file, only its corresponding private key can be used to unlock it and vice-versa. People

DOI: 10.4018/978-1-5225-9742-1.ch005

could use a public key to lock or encrypt a file, and they would be sure that the only person who could unlock it would be whoever held the matching private key. However, the issue after the establishment of public and private keys was identifying whether or not someone's private key and persona were appropriately matched. Malicious actors could claim to be another party and attempt to associate their own public key with the false persona in an attempt to redirect and steal sensitive information. Thus, public key infrastructure (PKI) was born in order to properly associate online identities with the correct public keys so that any online communication could be trusted to involve the correct parties.

However, with the pervasiveness and expansion of the Internet of Things, there comes new challenges for securing and authenticating the heavy flow of data generated by IoT devices. PKI's age has shown, and it has been unable to keep up with the demands of the IoT and Big Data era (Claeys, Rousseau, & Tourancheau, 2017). Big Data ecosystems require solutions that are scalable and resilient, two attributes that fail to be applied to traditional PKIs. Thus, in order to further secure the internet, a new method for identity verification over the web needs to be realized. The main issue with the currently outdated PKI lies with the Certificate Authority (CA) portion of the PKI (Doukas, Maglogiannis, Koufi, Malamateniou, & Vassilacopoulos, 2012; Gupta & Garg, 2015). CAs are the authorizing parties within a PKI; they validate and associate online personas with public keys by distributing and revoking digital certificates. These digital certificates act as ID cards for anyone that communicates over the internet, and they give a degree of assurance that the party one is communicating with is actually who they say they are. As of now, these CAs are the main points of failure within a PKI system; once any one CA is compromised, the whole PKI crumbles (Zhou, Cao, Dong, &Vasilakos, 2017). Furthermore, it is currently extremely difficult for a traditional CA to revoke an old identity. However, there are newer iterations of PKI that attempt to overcome these shortcomings; one of which is called Web of Trust (WoT). Another promising new solution marries the traditional PKI system with that of cloud and blockchain technology to overcome the weaknesses of the past (Tewari, Hughes, Weber, & Barry, 2018). Both of these systems are new ways of verifying identities that can pave the way towards a safer and more secure internet.

In this chapter, we explore the current state of PKI and its new incarnations that attempt to address the limitations of traditional systems. By doing so, we aim to answer the following questions: "How can new technologies such as blockchain be leveraged to improve traditional PKIs" and "What are the pros and cons of using one new solution over another". This chapter is extended from a conference paper which reported preliminary results (Khieu & Moh, 2019).

This chapter is organized in the following manner. First, it will establish background information surrounding the project and then cover research related to this area with a specific focus on other implementations of different PKIs. Afterwards, the methodology and reasoning behind our solution to the issues with the PKI model will be detailed. Subsequently, the chapter will cover the test results and performance comparisons between the different PKI models including our solution. Finally, the chapter will conclude with a summary and areas for future work.

RESEARCH OBJECTIVE

The objective of this research is to test and implement a Cloud-based blockchain PKI system, CBPKI, to provide Big Data applications with a scalable and persistent identity management system. In addition, the goal is to determine whether such a system can outperform traditional PKI models using metrics such as complete revocation time.