HKUST President's Cup Final Report

Vivian: Decentralized Global Naming and Storage System to Tangle

Submitted by:

TIAN Xiangan

Student ID: 20583620

Year of Study: 3

Supervised by:

Prof. TSOI, Yau Chat

Department of CSE

Department of Computer Science and Engineering

School of Engineering

Hong Kong University of Science and Technology

Vivian: Decentralized Global Naming and Storage System on Tangle

TIAN Xiangan
xtianae@connect.ust.hk

Supervisor: Prof. TSOI, Yau Chat
desmond@cse.ust.hk

***Abstract*—With the booming of distributed ledger technology (DLT) such as blockchain, many previous IT architectures can have alternative decentralized approaches for more secure, transparent, and immutable data storage. In this paper, we present the design and implementation of Vivian, a new decentralized global naming and storage system based on IOTA Tangle for re-decentralizing the current Internet service and building decentralized applications. Unlike the traditional Domain name Service (DNS), trust points like DNS root servers are removed and critical data bindings are secured by the distributed ledger. All the nodes in the system form a peer-to-peer (P2P) network for data sharing. The P2P network is established through Kademlia DHT, mDNS peer discovery and eventually consistency of data is ensured by Gossip protocol. In this system, users can own their application data directly rather than relying on the central authorities. The system has no single point failure and the nodes in the network do not need to trust each other. By using IOTA Tangle, a directed-acyclic-graph (DAG) structure distributed ledger, the system inherits its scalable, lightweight, and feeless characteristics and enables the possibility of application in Internet-of-Thing (IoT) services.**

I. Introduction

A distributed ledger is a type of distributed database that assumes the presence of nodes with malicious intentions. And distributed ledger technology (DLT) enables the realization and operation of distributed ledgers, which allows benign nodes, through a shared consensus mechanism, to agree on an almost immutable record of transactions with Byzantine failure tolerance (BFT) and eventual consistency [1]. Blockchain is one of the most well-known DLTs which was first implemented on Bitcoin. It proposed a simple but robust way for transaction data storage without relying on trust of third parties [2]. Blockchain also ensures improved security and anonymity of Bitcoin transactions compared with traditional electronic transactions. Since the introduction of Bitcoin in 2009, cryptocurrencies based on DLTs have made a great impact on financial sectors. People also discovered that the usefulness of DLTs is beyond exchange of currencies and significant adoption of DLTs were made in many other industries for other different services later on. Namecoin is the first altcoin (any cryptocurrencies that are not Bitcoin) for being the first to create its own blockchain separate from Bitcoin's [3]. The creation of Namecoin was inspired by the idea of BitDNS [4] and for establishing a decentralized domain name looking up system.

References

[1] A. Sunyaev, *Distributed Ledger Technology*, pp. 265–299. Cham: Springer International Publishing, 2020.

[2] S. Nakamoto and A. Bitcoin, "A peer-to-peer electronic cash system," *Bitcoin.–URL: https://bitcoin. org/bitcoin. pdf*, vol. 4, 2008.

[3] H. A. Kalodner, M. Carlsten, P. Ellenbogen, J. Bonneau, and A. Narayanan, "An empirical study of namecoin and lessons for decentralized namespace design.," in *WEIS*, Citeseer, 2015.

[4] F2b, "BitDNS and Generalizing Bitcoin." https://bitcointalk.org/index.php?topic=1790.0/, 2010. [Online; accessed 25-Feb-2021].