Vivian: Decentralized Global Naming and Storage System on Tangle Distribted Ledger

Overview

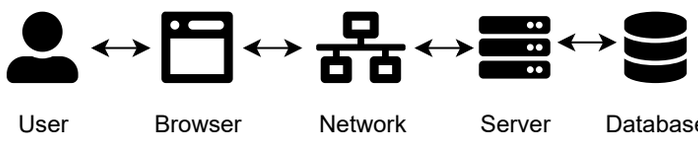
With the booming of distributed ledger technology (DLT) such as blockchain, many previous IT architectures can have alternative decentralized approaches for more secure, transparent, and immutable data storage. In this project, we propose the design and implementation of Vivian, a new decentralized global naming and storage system based on IOTA Tangle distributed ledger for re-decentralizing the current Internet service and building decentralized applications. The system has no single point of failure and the nodes in the network do not need to trust each other. Unlike the traditional Domain name System (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 user quires' routing. The P2P network is established through peer discovery protocols such as mDNS, Kademlia DHT and peers exchange data and achieve eventual consistency via Gossip protocol. We also provide a decentralized storage system which can hold user data securely without the control of central trust parties or revealing information to storage providers. By using IOTA Tangle, a directed-acyclic-graph (DAG) distributed ledger, the system inherits its scalable, lightweight, and feeless characteristics and most IoT devices have enough computational power to sign and send transactions. This extends the usage of Vivian to Internet-of-Thing (IoT) services for decentralizing IoT networks and enhancing IoT data security and privacy.

Problems

Problems of Current Internet Services

For most of the current Internet applications, data is stored in a centralized manner and users do not own the data by themselves. For instance, if users want to do actions like checking their emails or browsing the content of a website, first, they need to connect to the web servers via the Internet with web browsers, then the web servers retrieve the data from the database and then send it back to users. Usually, users' data is hidden behind service providers' application code. This kind of arrangement has been very successful as it is easy to implement. However, it is not ideal since:

1. Users must use the requested web user interface if they want to access their data.
2. The websites control the rules and access rights of the data.
3. The websites may snoop your data and sell users' information to others.
4. Illegal use of data by websites' employees for personal purposes.



Traditional user data arragement of Internet services

Problems of Domain Name System (DNS)

1. DNS root servers are central nodes of trust and failure, and cyber-attack such as DDoS towards them may lead to the whole system taken down.
2. These central points may also be exploited and misleading users into connecting to malicious websites.

Problems of Internet of Things (IoT)

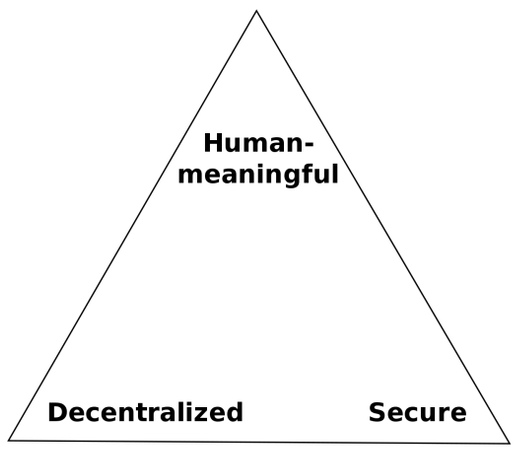
1. Inferior Scalability.
2. Large-scale data management.
3. Data security and data integrity.
4. Risk of centralized failure.

Problems of PoW Blockchains

1. Bad scalability
2. Low TPS
3. Massive energy consumption for PoW consensus.
4. Expensive transaction fees.

Solution

We introduce Vivian, a new decentralized global namingand storage system, which is a possible solution to the problems above. Vivian squares Zooko's Triangle trilemma andprovides a decentralized naming system, that allows users toregister human-meaningful names with binding information. Its storage layer also helps users to save their files in adecentralized and secure way. Unlike other blockchain based decentralized naming system, Vivian uses IOTA Tangle DL for critical data binding. Tangle is a lightweight and highly scalable DAG distributed ledger, which allows devices with poor computing power to write and send transactions on it. It extends Vivian's usage in IoT networks. In addition, the system is more environmentally friendly compared with other PoW blockchain applications as it does not require miners to do Proof-of-Work computations.



Zooko's Triangle trilemma of decentralized naming system

By TIAN Xiangan, Tommy (Year 3, COMP) Supervised by Prof. TSOI, Yau Chat, Desmond (CSE)

Vivian: Decentralized Global Naming and Storage System on Tangle Distribted Ledger

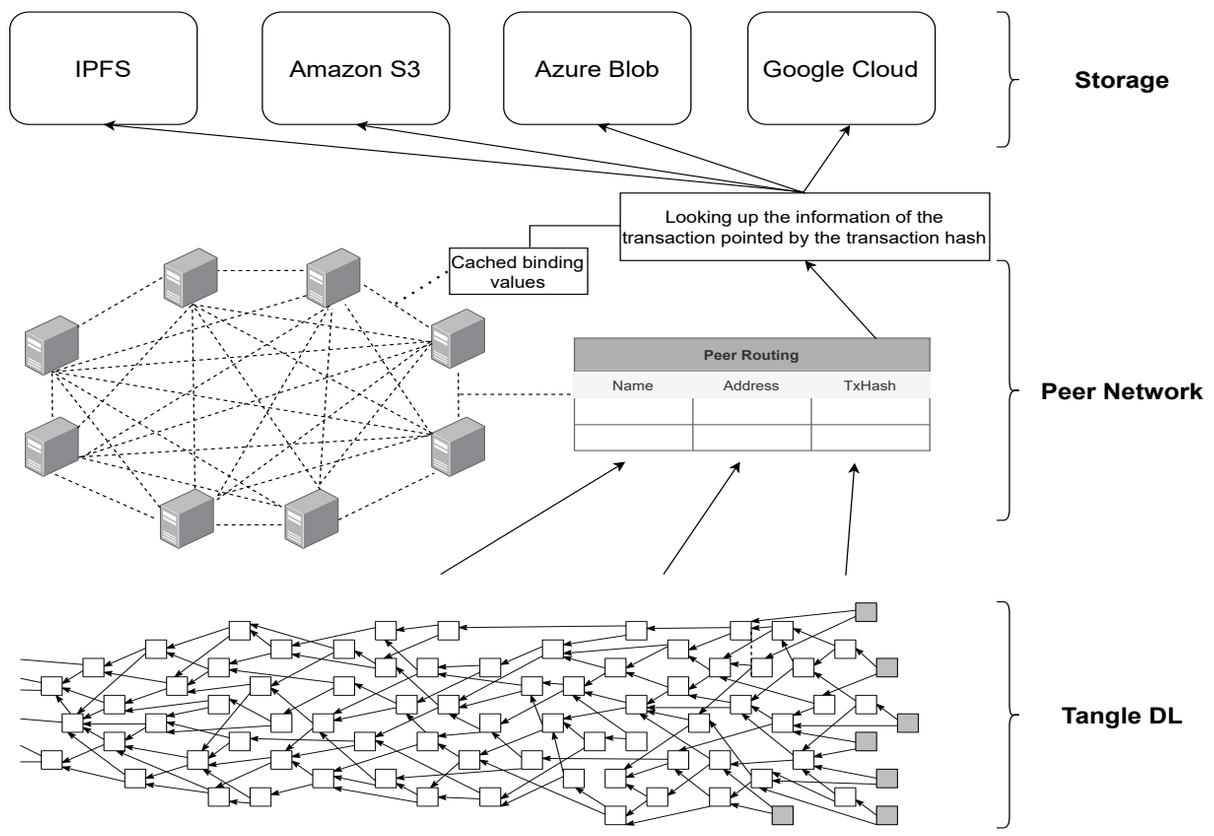
Design

Design Goal

1.Decentralized Naming and Look-up. End-users can register for and bind values to human-meaningful names and look up the values of names without relying on the trust of central authorities.
2.Decentralized and Secure Storage. End-users can store their data in a decentralized manner. Besides, users can control the access rights of their data.
3.IoT Device Supported. The whole process like registering a name, looking up a name, and file handling should not be energy-hungry or hardware resource hungry. They can be accomplished by devices with limited hardware resources such as Raspberry Pi.

Three Layer Structure

1. Tangle DL: Tangle distributed ledger layer records critical data bindings.
2. Peer network layer handles user queries and help user find the binding value of the names quickly.
3. Storage layer stores user data under users' control securely and the storage providers cannot tamper with the data.

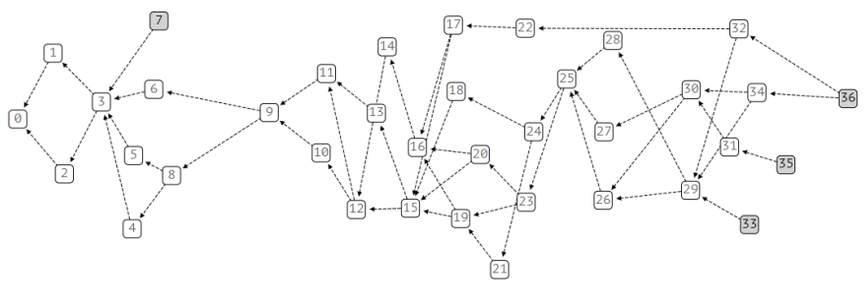


Vivian structure

Implementation

Tangle Distributed Ledger

A DAG distributed ledger with following advantages:
1. High Scalability 2. Feeless 3. Lightweight

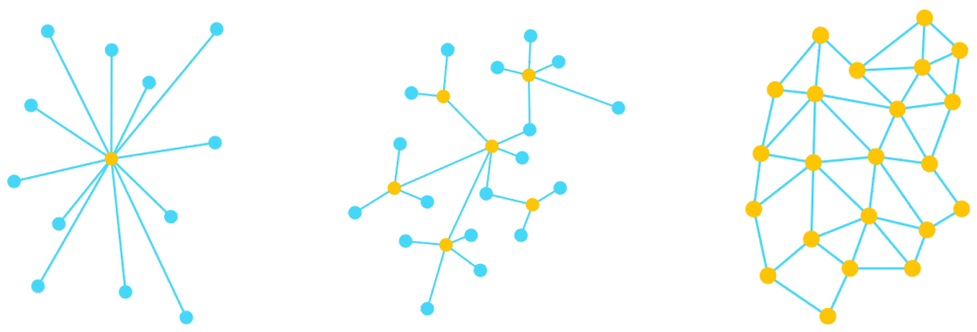


Tangle DAG structure

Peer Network

Peer Discovery:

1. Bootstrap 2. mDNS 3. Kademlia DHT random walk



(1) (2) (3)

Network structure after each peer discovery precedure

Peer Communication:

Gossip Protocol. a procedure or process of computer peer-to-peer communication that is based on the way epidemics spread

Applications

Decentralized Website. Users can build and maintain their website through Vivian decentralized naming system and storage layer. Compared with traditional websites, decentralized websites are censorship-resistance (only the owners can censor or modify the the content of their websites), more robust (it is much more difficult to take them down or DDoS), and private (the owner of the decentralized websites can be anonymous).

Identity Attachment. Users can attach identity information such as GPG public keys, email address, cryptocurrency addresses that are not human-meaningful or easy to memorize to name they like.

Enhance IoT Scalability and Privacy. Inferior scalability, server failure, large-scale data management, and data privacy are four of the weaknesses of the current IoT network implementation. Traditionally, all the data is transmitted from a device or an object to central cloud servers where it is stored and analyzed. If the centralized server fails, the whole network is at risk of taken down. As more and more devices joining IoT network, scalability issues are getting worse. Also these devices are producing massive amounts of data including sensitive information, and large-scale data management and data privacy issues are becoming more severe. Vivian and IOTA can help to decentralize the current IoT network, and data can be stored on Tangle DL or storage layer provided by Vivian. This improves the scalability and data privacy of IoT services.

By TIAN Xiangan, Tommy (Year 3, COMP) Supervised by Prof. TSOI, Yau Chat, Desmond (CSE)