BLOCKCHAIN TECHNOLOGY LAB

(20CP406P)

LAB ASSIGNMENT - 4

B.Tech in Computer Science and Engineering Dept.,

Pandit Deendayal Energy University,

Gandhinagar

Name: Parth Nareshkumar Patel

Roll No.: 19BCP091

Branch: Computer Engineering

- **Aim:-**

Understand KSI(Keyless Signature Infrastructure**)**

- **Introduction:-**

- KSI is a method and a globally distributed network infrastructure for issuing and verifying KSI signatures.
- Unlike traditional digital signature approaches, e.g. Public Key Infrastructure (PKI), which depends on asymmetric key cryptography, KSI uses only hash-function cryptography, allowing verification to rely only on the security of hash functions and the availability of a public ledger commonly referred to as a blockchain.

KSI Blockchain

- A blockchain is a distributed public record of events; an append-only record of events where each new event is cryptographically linked to the previous. New entries are created using a distributed consensus protocol.
- The KSI blockchain overcomes two major weaknesses of traditional blockchains, making it usable at an industrial scale:

1. **Scalability:**
   - One of the most significant challenges with traditional blockchain approaches is scalability
   - they scale at O(n) complexity i.e. they grow linearly with the number of transactions. In contrast the KSI blockchain scales at O(t) complexity – it grows linearly with time and independently from the number of transactions

2. **Settlement time:**
   - In contrast to the widely distributed crypto-currency approach, the number of participants in the KSI blockchain spread consensus protocol is limited. By limiting the number of participants it becomes possible to achieve consensus

synchronously, eliminating the need for Proof of Work and ensuring settlement can occur within one second.

Contrasting KSI to Bitcoin and RSA

	KSI	Bitcoin	RSA
Scalability	global, linear to time	global, linear to a number of transactions	local
Settlement time	under 1 second	non–deterministic, 5–15 mins	under 1 second
Data privacy	data never disclosed	data added to blockchain	data never disclosed
Key management	n/a	n/a	yes, necessary
Quantum threat	not vulnerable	vulnerable	vulnerable

Scalable blockchain-backed authentication for electronic data

A user interacts with the KSI system by submitting a hash-value of the data to be signed into the KSI infrastructure and is then returned a signature which provides cryptographic proof of the time of signature, the integrity of the signed data, as well as attribution of origin i.e. which entity generated the signature.
The benefits of the KSI:

Massive Scale:

The KSI signatures can be generated at an exabyte scale. Even if an exabyte (1,000 petabytes) of data is generated around the planet every second, every data record (a trillion records assuming 1MB average size) can be signed using KSI with negligible computational, storage, and network overhead.

Potability:

The properties of the signed data can be verified even after that data has crossed geographic or organizational boundaries and service providers.

Quantum Immunity:

The cryptography behind the KSI signatures ensures that they never expire and remain quantum immune i.e. secure even after the realization of quantum computation.

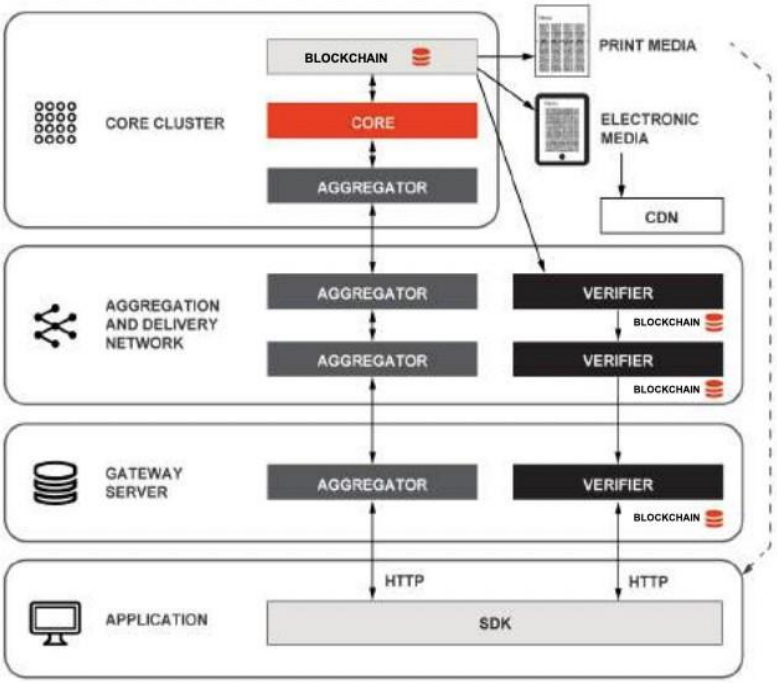
Independent Verification:

The properties of the signed data can be verified without reliance or need for a trusted authority.

Data Privacy:

KSI does not ingest any customer data; data never leaves the customer's premises. Instead the system is based on one-way cryptographic hash functions that result in hash values uniquely representing the data, but are irreversible such that one cannot start with the hash value and reconstruct the data – data privacy is guaranteed at all times.

KSI Service Infrastructure:-



Core Cluster:

A component responsible for managing the KSI blockchain.

Aggregation Network:

A component providing scale, redundancy, and global reach for the KSI service delivery network.

Gateway Server:

A hardware or software component at the customer premises providing access to the KSI service.

Application Integration:

Guardtime provides fully featured SDK-s for C, Java and .NET to facilitate KSI service integration to customer applications.

.