BLOCKCHAIN TECHNOLOGY LAB

(20CP406P)

LAB ASSIGNMENT - 4

B.Tech in Computer Science and Engineering Dept.,

Pandit Deendayal Energy University,

Gandhinagar

Name: Mire Kishorkumar Patel

Roll No.: 19BCP080

Branch: Computer Engineering

Lab Assignment 4

Aim: Understanding and Exploring KSI.

Introduction:

KSI - Keyless Signature Infrastructure:

- 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.

Keyless Signature Infrastructure (KSI) technology was initially developed in 2007 with the goal to impart a tag on any digital file that would forever be effective in determining its authenticity. Exploiting a mathematically derived artifact of a file called a hash along with the hashes of other files created in the same time increment, and combining them in a mathematically known manner called a hash tree or a Merkle Tree accomplish this. This process cryptographically links all the artifacts of the files created or modified in that time increment and creates a top root hash that can be used in a proof that shows the contribution of every file. Once this top root hash is determined, it is then combined with the top root hashes from previous time increments in a hash calendar. Combination of all the artifacts for a particular instant in time can be summarized on a publication code. The steps taken in the mathematical sequence of combining the hashes is well defined and repeatable. The process and path used to move from initial hash to the publication code is defined in a

unique digital KSI signature (approximately 2 kilobytes). In this implementation the artifacts from the files in the current time increment are cryptographically linked to all the artifacts of files brought into these processes since it was initiated and a summary is provided in the publication code. This is one instantiation of what has been called a blockchain.

To verify the authenticity of any digital file, one must have the file under test. With the hash of the file under test and the signature attributed to the original file, verification is accomplished by using the hash of the file under test as the starting hash and processing it through the Merkle Tree with the data from the original signature and comparing the result to the publication code. There is no mystery to the approach, no puzzles to be discovered, the process follows the published KSI process (the Merkle Tree) using the KSI signature and comparing the result to a published result. If the process generates the same publication code, it is identical to the original file. If it does not, then it is a forgery or an altered version.

The top root hashes of every time increment are stored in the KSI infrastructure such that it is always available for verifying signatures. This storage scales at approximately 2 gigabytes per year, scaling with time, not with number of items signed or processed.

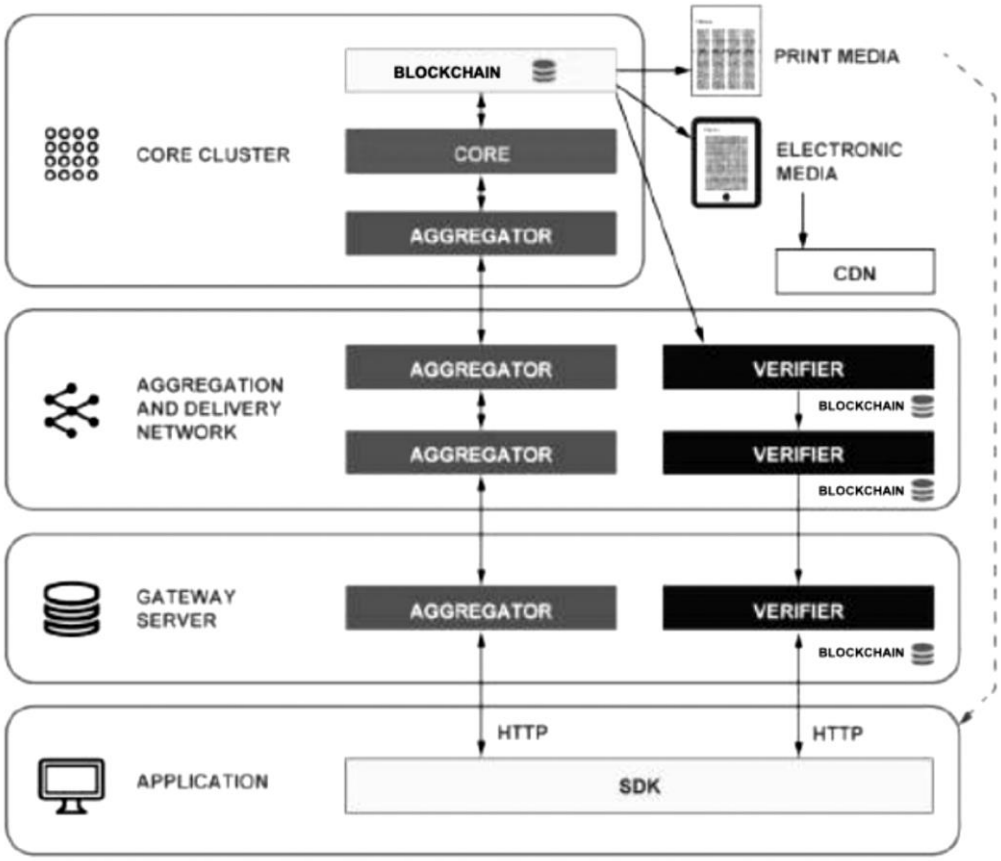
Note that a hash is a one-way function such that a file can be hashed but there is no mathematical process that allows one to re-create the file from a hash. Once the initial file is hashed, all other processes have no insight into the content of the original file and the file content is not widely distributed. Only the hashed artifacts of the file are widely distributed. This enables anyone to verify the contribution of a hash at a point in time without having to be exposed to the potentially sensitive data in the original file (e.g., personal medical data).

The information derived from a KSI signature means the asset's chain-of-custody information (pedigree), creation time, and authenticity information remains undisputable and is subsequently verified as truth without trusting or solely relying upon an administrator or a shared secret (such as a key or Public Key Infrastructure (PKI) credential). Instead, KSI uses a 'proof-based' method to accomplish authentication and our signature is portable across any computing platform. KSI signatures are based on mathematical proofs and keyless cryptographic functions approved by the European Union (EU) and National Institute of Standards (NIST).

KSI addresses the need to prove data integrity and detect changes in data authenticity at rest and in motion. It is a blockchain technology, which provides massive scale data authentication without reliance on centralized trust authorities.

KSI forms a unique calendar hash chain (CHC) that is a distributed database across the infrastructure. Records can only be added to the database, never removed, with each new record cryptographically linked to all previous records in time. New records can only be added based on synchronous agreement or 'distributed consensuses of the parties maintaining the database. Since records are cryptographically linked, it is impossible for one party to manipulate previous records without breaking the overall consistency of the database.

The KSI Infrastructure:



The KSI infrastructure consists of a distributed network of Black Lantern Security Appliances configured as cores, aggregators, and gateways. The first layer of aggregation servers are the gateways which are responsible for collecting and processing requests from clients and then sending the aggregate request to the upstream server. The gateway is the customer facing component of the infrastructure and delivers KSI services to the clients.

The network aggregates the hash values and distributes the signatures. Each aggregation server processes requests from the servers below it, adds them to a hash tree and sends the local root hash to the next higher-level server. The hierarchy of aggregation servers creates the global hash tree for each round. The verification network (a part of the aggregation network) provides widely

witnessed access to the state of the calendar and the history of root hashes used in the verification solutions.

The core cluster operates a distributed state machine which sits at the top of the aggregation network and manages the calendar. It calculates the top root hash at one-second intervals (a round) and votes upon (through distributed consensus) and promotes the top root hash to the CHC. The core is responsible for agreeing upon the top root hash for each aggregation period, which it then stores in the calendar database, and returns the result to the aggregation network. The regularly spaced rounds used in the aggregation and core processes produce an accurate measure of time, which is embedded into the KSI 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.

- **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.

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

- **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 has values uniquely representing the data, but are irreversible such that one cannot start with the hash value and reconstruct the data - data privacy is always guaranteed.

- **Independent Verification:**
  The properties of the signed data can be verified without reliance or need for a trusted authority.

Conclusion:

There is no other sector where corruption-free data matters more than in Healthcare/Healthcare IT. Guard time Federal's KSI Blockchain-based data integrity and assurance capabilities can be deployed to complement existing healthcare solutions, not to replace them, thus making implementation affordable. The value of KSI digital signatures is how it is applied to a customer's problem. Any type, format, or size of data can be signed and its integrity documented for use. This capability allows KSI to directly link to the Nationwide Interoperability Roadmap and healthcare related objectives. The KSI signing and verification process currently in use today, is scalable and controlled and easily integrated in systems for interoperability. The infrastructure using Black Lantern Security Appliances provides security from many threats (cyber and physical attack vectors) to offer non-repudiation, proof of integrity, irrefutable identity, irrefutable event time, longevity, and pedigree. This characteristic can be used to mitigate or prevent insider threats, fraud, or unwanted data loss. Some healthcare related use cases have already been developed and can demonstrate how to provide integrity for event logging, software authenticity, and data transactions. This leads to many opportunities

for auditing, monitoring, configuration management, change detection and reporting on the integrity of data in development processes, engineering, operations, and maintenance of many systems in commercial, military, and healthcare markets.