International Journal of Recent Engineering Research and Development (IJRERD)
ISSN: 2455-8761
www.ijrerd.com || Volume 03 – Issue 07 || July 2018 || PP. 15-24

Block chain based KSI for delivering governmental services in democratic nations

Vedna Sharma
Junior Research Fellow
Institute of Technology Management
(Defense Research & Development Organization)
Landour Cantt. Mussoorie Uttarakhand (India)

Abstract: There are various challenges that government organizations are addressing naturally characterized by transparency and security in government records, improved confidentiality and integrity of data, secure transactions and information security. Government has to be choosing the design that best fits for balancing security and central control with the convenience and opportunity of sharing information or data between organizations and individuals.

Government Organizations are also investing in digital technologies to support their goals. Significant investment in technology and efforts has yielded great progress in growth, efficiency & demand of organizations. Block chain stands out as a technology in which various organizations see potential to solve these challenges by implementing strong authentication, data encryption and digital signature.

Keywords: Blockchain, Digital Signature, Hashing, public key Infrastructure, Keyless Signature Infrastructure and Governmental Services

1. Introduction

Blockchain is decentralized technology that is built on the model of offering security and trust. Blockchain technology have the potential to help governments to collect taxes, deliver benefits, issue passports, record land registries, assure the supply chain of goods and generally ensure the integrity of government records and services. Blockchain technology can simplify the management of trusted information, making it easier for government agencies to access and use critical public-sector data while maintaining the security of this information. Block chain allows digital information to be distributed but not copied.

A block chain is an encoded digital electronic ledger that is stored on multiple computers in a public or private network. It is a transparent technology since code is open and accessible to anyone but impossible to manipulate. Block chain can help agencies to digitize existing records and manage them within a secure infrastructure. There are a number of block chain tools and technologies that government agencies can implement today to secure critical data and improve the management of records associated with property ownership and incorporation.

This paper is primarily focused on implementation of block chain based keyless Signature Infrastructure (KSI) for authentication, availability, confidentiality and integrity of public sector data in democratic setup. Keyless signatures are an alternative solution to traditional PKI signatures.

Section 1 contains Introduction part of research work. Challenges in delivering governmental services in democratic setup are defined in Section 2. A case study is done on development and adoption of Blockchain in government or public sector in Estonia & Dubai. is defined in section 3. Section 4 explains Sectors exploring potential applications of blockchain technology. Section 5 describe implementation of blockchain , proposed model and technical overview of blockchain and section 6 define discussion & conclusion.

2. Challenges in delivering governmental services in democratic setup

Although democracy has been accepted as the best form of Government in the modern world. Yet it has its own problems. Democracy means 'government of the people, for the people, and by the people'. It means democracy is not limited to just a process of election, but also fulfilling social and economic aspirations of the people.

A system can be termed as a genuine and comprehensive democracy only when it fulfills both political and socio-economic aspects of people's participation and satisfaction. There may be two major categories:

(a) Political conditions
(b) Social and economic conditions

The fulfillment of the first leads to political democracy and the second as social democracy. The growing public dissatisfaction with corruption in public life has loose the trust of people from government services. Corruption is the major issue in the development of any democratic nation and developing countries. Various government agencies

such as police, judicial services, land administration, education, tax and health services are major fields in which need of transparency, accountability and integrity to overcome the corruption. One major form of corruption is large-scale corruption in the form of huge bribes on major government contracts, particularly on large imports of arms, an inherently non-transparent area, subject to national security considerations; bulk commodities; large infrastructure contracts; allocations of natural resources, such as minerals; or the telecom spectrum, all of which are controlled by politicians [11].

Another major form of corruption is direct theft of government funds from development programmes such as irrigation and roads, from social and anti-poverty programmes, from publicly funded loans to the poor, and the diversion of price controlled goods, that are in short supply, for sales at higher market rates. These involve both bureaucratic and political corruption and overlap with cultivating electoral constituencies. This form of corruption, that is, directs embezzlement of government funds and materials. There is also large-scale corruption in government recruitment, postings and transfers to 'lucrative' positions, those in which coercive bribes can be extracted. The rate of bribes ranges from 10—20 percent of the legal sums involved for various services.

Blockchain application on the public sectors and on under-developed countries has the potentials to root out corruptions and lift those countries out of poverty. Without interfering the data governance and privacy issues, blockchain technology always lead to a socio-economic benefit. Its implementation on the developing or under-developed world will not be realized on a large scale anytime soon due to the resistance of the existing leadership and lack of infrastructure.

This technology can be used as anti-corruption measures to fight against corruption and technology have often been an effective tool of improving integrity.

Blockchain technology addresses every transaction's authenticity by confirming the parties involved, the time and date of transaction as well as the contents. If a transaction contains fraud information due to corruption or forgery, then it is not validated due to the consensus protocol and, therefore, transaction cannot take place. As such, the blockchain technology can be an effective tool to root out corruptions from having a transparent view on every transaction.

The U.S Postal Service Office of Inspector General (OIG) examined how the blockchain technology could impact the Postal Service's businesses (USPS 2016)[14]. Government and financial institutions can use the technology as a means of combating financial crime such as money laundering and tracking any fund transferred for criminal activities such as drugs trade or terrorism. With the use of the technology, every transaction can be recorded without manipulation, making the ultimate destination transparent.

3. Case Study: Development and adoption of Blockchain in Government or public Sector

In the government sector, there is need to increase the transparency and accountability of government's legitimacy processes rather than prioritizing confidentiality.

Estonia is one of the world's leading information Society. Estonia aims to propagate digital services and technical implementation to support digital interaction. After suffering a national-scale cyber attack in 2007, Estonia recognized that a new approach was needed to restore and guarantee trust in digital systems. In 2007 a team is assigned by Estonian Government, in which network architects, software developers and security specialists and cryptographers designed a digital signature system that could provide Exabyte-scale real-time authentication. Estonia's experience with the use of blockchain technology in government provides a useful benchmark for comparision with other nations.

In Estonian application of blockchain technology, Keyless Signature Infrastructure (KSI) plays main role. KSI is a blockchain technology designed in Estonia and used globally to make sure networks, systems and data are free of compromise, all while retaining 100% data privacy.

In October 2016, Dubai launched a city wide blockchain strategy with the objective of becoming the first blockchain powered city, driving the future economy by 2020. This ambition sees Dubai Government leading innovation and building the enabling ecosystem for it to thrive in both the public and private sectors [4].

A KSI blockchain is a distributed public ledger – a database with a set of pre-defined rules for how the ledger is appended by the distributed consensus of the participants in the system. With KSI Blockchain deployed in Estonian government networks, history cannot be rewritten by anybody and the authenticity of the electronic data can be mathematically proven. It means that no-one – not hackers, not system administrators, and not even government itself – can manipulate the data and get away with that. The KSI blockchain is used for both internal and external processes to maintain integrity of records and enable detection of both intentional and unintentional modifications.

The Estonian information society is based on the basic principles which are decentralization, open platform, interconnectivity and open ended process.

There are various State Agencies that are currently implementing KSI Blockchain technology within their various domains. In Estonia, X-Road an interoperability platform is used for integrates different interfaces such as in

security services and registration services. X-road platform is used for various government e-services in healthcare, Business, tracking information system and digital court system and official state Announcements [3].

3.1 The blockchain strategy is based on three pillars

1. Government Efficiency Implement blockchain technology in applicable government services.
2. Industry Creation Support the creation of a blockchain industry through providing an enabling ecosystem that empowers start-ups and businesses.
3. Local and International Thought Leadership Lead the global thinking on blockchain technology and become the hub for blockchain intellectual capital and skill development [4].

4. Sectors exploring potential applications of blockchain technology

Banking System

The global payment settlement system is still based on correspondence banks or on a network of clearing bodies. There is only limited digitization and standardisation due to which settlement periods and costs are corresponding high. Blockchain technology could remedy such problems. Blockchain would remove the need of third parties and increase security and transparency [5].

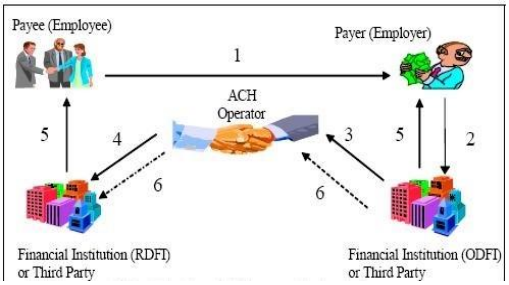

Figure 1(a) : Traditional Model (2-3 days)

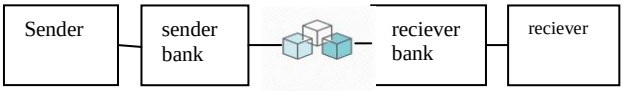

Figure 1(b) : Blockchain Model (Minutes)

Election System

Voting system in election process are major unresolved issue of corruption in democratic and under developed countries. For example by inaccurate voting for multiple registrations, the election result may not always reflect the public opinion but it is subject to manipulation by a corrupted authority.

In such circumstances, the blockchain technology ensures that every eligible vote is counted accurately without any manipulation and this can be a huge step towards true democracy.

Property & real-estate

Corruption on the property and real-estate market is another unresolved issue for some countries. Honduras is declared as one of the most corrupted countries in the world, ranking 123rd on the Corruption Perceptions Index by Transparency International due to the corruptions occurring on land registries the government of Honduras partnered with a blockchain start-up to develop a system that kept the land record on a transparent and unhackable blockchain platform. Apart from being transparent, users of the blockchain system could inspect a search for any property records in real-time without any cost.

Foreign Direct Investment (FDI)

There is also need transparency among NGOs and charitable organizations to eliminate the misappropriation of funds by keeping a public ledger of all financial transactions involved in the charitable activities. Implementation of Blockchain technology would be valuable to international organizations such as the World Bank in tracking where the loans are being spent within the borrowing countries' borders.

Cyber Security

Being a digital society means exposure to cyber threats. Blockchain is a scalable technology used to ensure integrity of data stored in government repositories and to protect its data against insider threats.

Block chains solve challenging problems in data science by using in cyber security. Blockchain technology has ability to improving data integrity and to prevent DDoS attacks to enabling safer IOT devices. Security that blockchain provide is not dependent on secret and trust. There are no passwords to be exposed. There are various use cases for blockchain in cyber security as given below:

1. Improved confidentiality and integrity of data.
2. Security of private information exchanged in chats, messaging apps and through social media.
3. Security of domain name system (DNS) from criminal attack and hacking
4. Elimination of the risk of false key propagation and enable application to verify the identity of people.
5. Security of IOT devices with authentication

5. Implementation of Blockchain

5.1 Blockchain data Structure

Block chain basically combines three existing technologies. Which are private key cryptography, peer to peer network (P2P) and blockchain protocols. The main purpose of cryptography in blockchain technology is to create a secure digital identity reference. Identity is based on possession of a combination of private and public cryptographic keys. The combination of these keys creating an extremely useful digital signature.

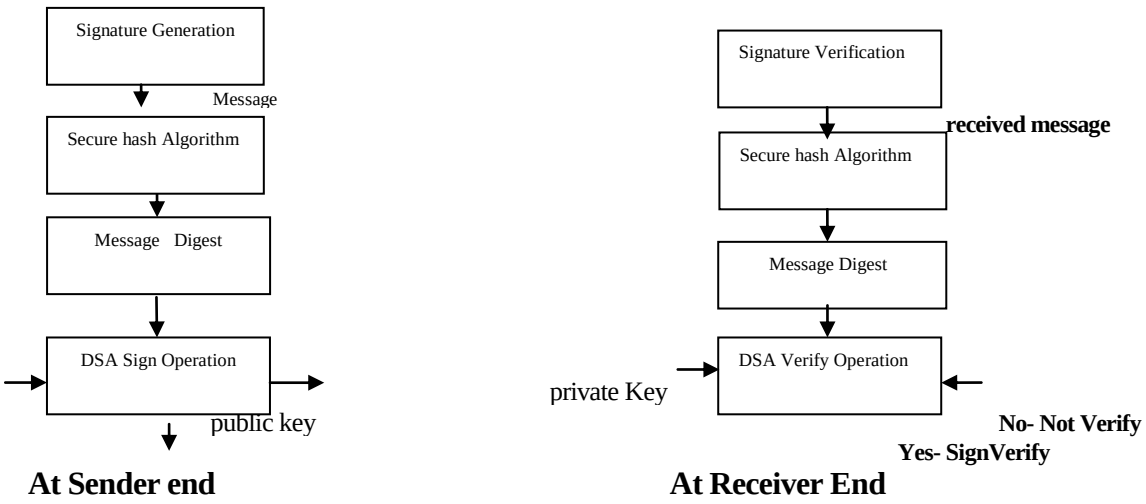

Figure : 2 Digital Signature Cryptographic technique binds a person or entity to digital data

Each block containing a hash value of current block, hash value of previous block and relevant information that broadcast to all nodes in peer to peer network.

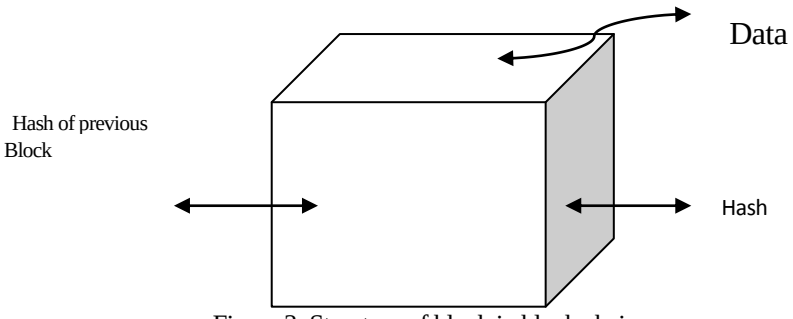

Figure 3: Structure of block in block chain

The amount, type and verification can be different for each block chain. Therefore set of rules are assigned to verify what is and is not a valid transaction or valid creation of blocks are block chain protocols.
Block chain basically works on the linked list data structure. It is a database which is composed of blocks i.e. group of records, where each blocks containing a cryptographic link to the previous block to form a chain. Data contained in each block processed to fit in a block through mining. Each block could be identified using digital fingerprint using a cryptographic hash value. All data blocks could be connected by using linked list data structure as in diagram.

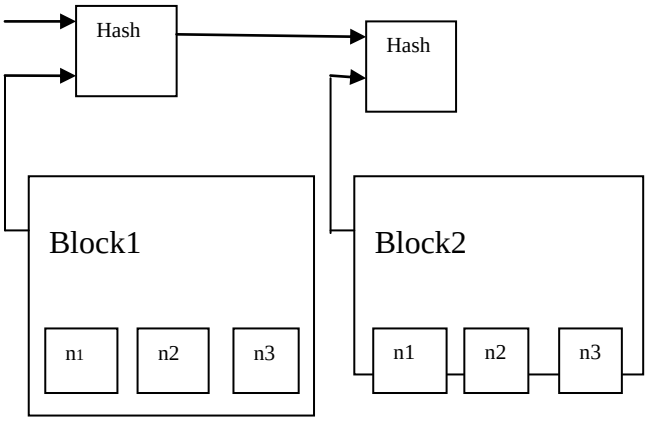

Figure 4: Block structure of Blockchain

5.2 Securing Communication using Public Key Infrastructure

Public key infrastructure is the public key cryptography that secures data messaging applications, strong authentication, confidential emails, e-commerce, internet banking and other form of communication. In public key infrastructure most of the implementations rely on the Certificate authority (CA). In PKI arrangements public keys are bind with respective identities of entities (like people and organizations). The binding is established through a process of registration and issuance of certificates at and by a certificate authority (CA).

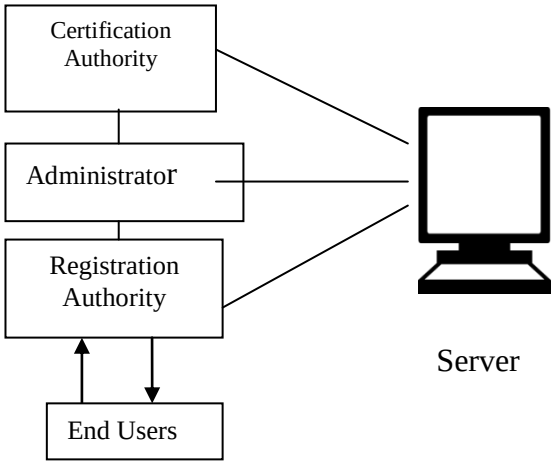

Figure 5: Central certification authority: single point of failure in Traditional PKI

5.3 Comparison of Block chain PKI with KSI

As shown in above dig. In Simple Public key Infrastructure there is a single point of failure that there are chances of hack data from the main server. To overcome this failure an emerging approach for PKI is to use the Block chain Technology i.e. Keyless Signature Infrastructure (KSI). Block chain technology aims to provide a distributed and unalterable ledger of information. Increasing the security of the system is done by eliminating the need of a single point of trust or certificate authority.

A block chain KSI has various advantages over a traditional PKI such as given below:

1) Block chain based KSI is used on top of existing security of technology.
2) There is no need to signed certificate which reduces the time it takes to transmit a certificate backed by a CA certificate chain.
3) Validation of a certificate and its CA certificate chain is trivial. A block chain being a "distributed ledger", the verifier has a local copy of the entire block chain and looks up hashes of certificates in block chain stores in the local copy, without network access. No signatures need to be verified.
4) Block chain PKI solves a longstanding problem of traditional PKIs by not requiring the use of a service that issues certificate revocation lists (CRLs) or responds to online certificate status protocol (OCSP) queries.

5.4 Proposed Integrated Model of KSI Blockchain

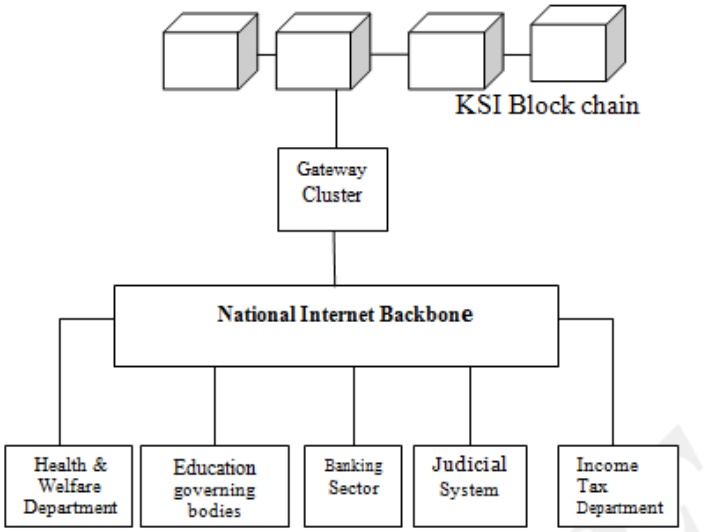

Figure 6: Integrated Model of KSI Blockchain

Keyless Signature Interface (KSI) occupies a central place in application of blockchain technology. This technology can be integrate into key government registries, official announcements, business registry, digital court files and all government sectors data. KSI Blockchain is basically used to provide a signature service. Customer transmits the asset's hash value and a token is receives in return that proves user participation in blockchain which create "proof of existence" for digital information. In KSI service original data never leaves customer premises, only hash value sent to the KSI service. The main advantage of this service is that signatures can be verified independently with high level of system scalability support.

Internet Backbone act as interoperability platform which is use to integrates all interfaces of various department or organizations and security services and can be work as technical backbone for all e-services in public sectors. Basic security offer by Internet backbone are integrity, high availability of services, confidentiality data exchanged and authenticity.

The X-road supports various government e-services in various areas such as in education bodies, in health & family welfare departments for electronic health records and e-prescription system , in home affairs departments for judicial and police functions, banking sectors, in various registration services such as electronic taxes declaration, validations of registered vehicles and driving licenses and exchanges of documents amount government agencies.

5.5 Technical Overview of the Keyless Signature Infrastructure (KSI)

Keyless Signature (KSI) is a Hash-tree based Block chain technology. The KSI technology is basically introduces three main components:

1.Aggregation networks
2. Core clusters
3. KSI gateways

Aggregation Networks

Aggregation networks are one of the main part of the KSI system. KSI technology is basically based on the hash values. These networks are essential part of KSI subsystem which is used to create Hash trees from all incoming requests. The top hash value of each hash tree is sent upstream for further aggregation into the core clusters. The aggregators work in rounds of equal time intervals. An aggregator delivers response to all aggregators at lower levels together with its hash tree's all hash paths after receiving a response from upstream components and then it used to verify the signature token.

Core Clusters

Core clusters are also one of the main components of KSI. These are distributed synchronized systems which are responsible for achieving consensus on the top value hashes from aggregation periods. Core clusters permanently stores the top hashes in the calendar database and return them as a part of signature token to the aggregation network. It is also responsible for time synchronization and used to represents the issuing time for each signature token.

KSI Gateways

KSI based gateways used as interface for different applications that uses the KSI block chain. Either Gateway must not be treated as a trusted party. The gateway used to implement first level of aggregation to predict the workload and avoid to extra bandwidth channels. The gateways also implement an extender service that provides signature verification. This service has access to a fresh copy of calendar database and help to find missing hash value which is necessary that is necessary to build complete hash chains from signed data to latest published hash value.

5.6 Working methodology of KSI

KSI based Blockchain technology is basically relies on Hash trees, which is data structure that is used to protect the integrity of documents using cryptography based hash functions. Hash tree stores the hash value of document of user i.e. cryptographic hash value. In return user receives a token as a receipt for proof of existence of data. That signature token is used as initial point to construct the path for hash tree. Hashes of various documents are store as leafs in hash tree. Aggregated hashes are used to generate hashes from the lower layer as shown below in diagram.

Keyless signatures are an alternative solution to traditional PKI signatures. The word keyless doesn't mean that no cryptographic keys are used during the signature creation. The signatures can be reliably verified without assuming continued secrecy of the keys but Keys are still necessary for authentication. Keyless signatures are implemented in practice as multi-signatures, i.e. many documents are signed at a time. The signing process involves the following steps:

1) **Hashing**: The documents to be signed are hashed and the hash values are used to represent the documents in the rest of the process.
2) **Aggregation:** A global temporary per-round hash tree is created to represent all documents signed during a round. The duration of rounds may change
3) **Publication:** The top hash values of the per-round aggregation trees are collected into a hash tree known as hash calendar and the top hash value of that tree is published as a trust anchor. To use such signatures in practice, one needs a suitable Keyless Signatures' Infrastructure (KSI) instead of PKI for traditional signature solutions. Such an infrastructure consists of a hierarchy of aggregation servers that create the per-round global hash trees. Gateways i.e. First layer aggregation servers are responsible for collecting requests directly from clients; every aggregation server receives requests from a set of lower level servers, hashes them together into a hash tree and sends the top hash value of the tree as a request to higher-level servers. The server then waits for the response from a higher-level server and by combining the received response with suitable hash chains from its own hash tree creates and delivers responses for each lower-level server[2].

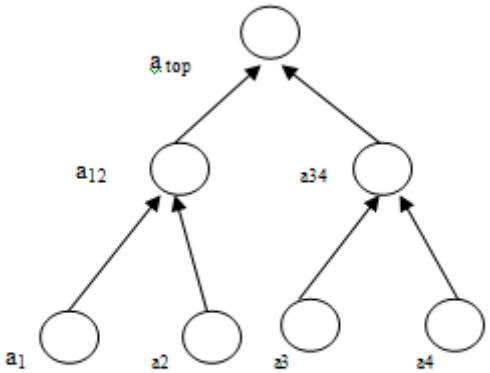

Figure 7: Example: Hash tree in KSI Service

As shown in above figure a_1, a2, a3, a4 are documents which are stored in hash tree as leafs. a_{12} and a_{34} are intermediate nodes which are generated by hash function. a_{top} is the top hash value of hash tree.

Now to check or verify the a_2 document compare the value of x_3 with the $a_{top,\ if}$ a_{top}= x_3 then it is verified that document a_2 is original and not modified as shown in below figure.

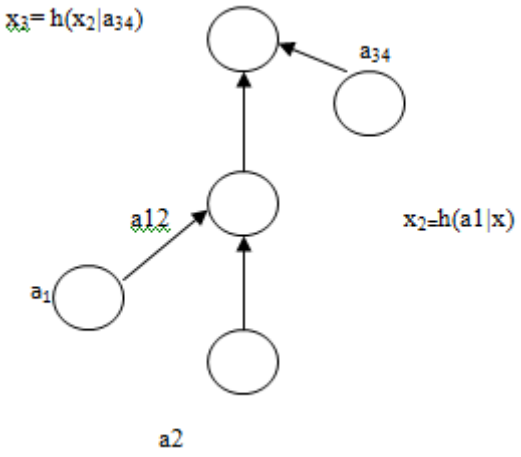

Figure 8: Verification of document in hash tree

5.7 The main architecture of KSI's aggregation networks

The application performs the first hashing step, which also generates request for sign in. That signing request is sent to gateway i.e. a system component which delivers the service to end users. Gateway forwards signing request to the aggregation network and performs initial aggregation of the request received in aggregation cycle-then its aggregate request sends to upstream aggregation cluster. All requests are aggregated through multiple layers of aggregator servers and globally top hash value is stored in core cluster [2] .

Once the top hash value reaches the core cluster then it stored in the calendar database and distributed through the calendar cache to the extender service. The core cluster is also responsible for reaching consensus among servers. The values from the calendar database are also available from calendar cache and cache is then used by extenders during verification phase.

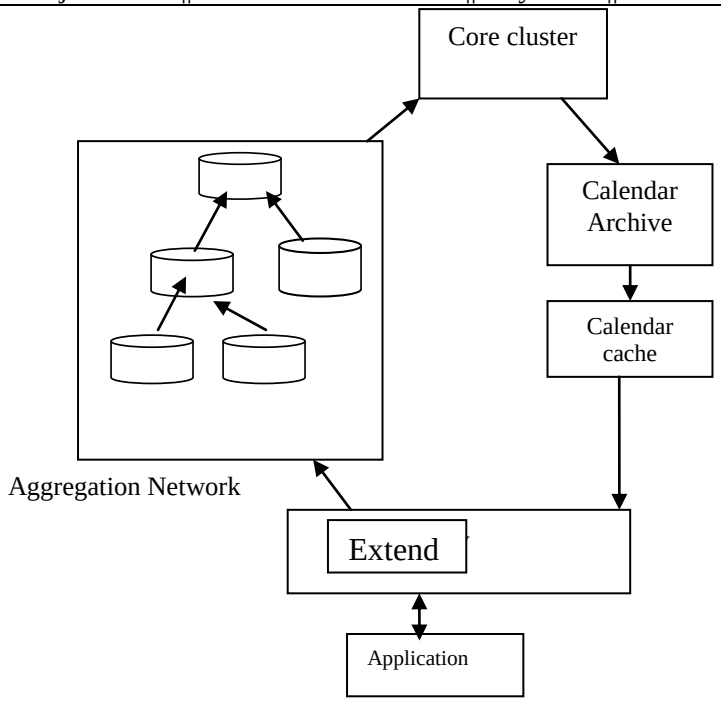

Figure 9: High level system architecture for KSI System

6. Discussion & Conclusion

The blockchain technology that containing various application areas is surely an innovative technology. This paper reviewed how this technology can be used in development of democratic countries to achieve next level of integrity by controlling the corruption. Either blockchain technology blockchain technology is not a universal solution that will resolve all corruption related issues we are facing. Also adoption of this technology to the developing or under-developed countries will not be as soon possible due the lack of infrastructure and resistance of the existing leadership. From the Estonia case study we reached the conclusion that the use of blockchain technologies in public life and governmental affairs offers notable benefits. There are also notable challenges yet. The biggest challenge is to understand the overall security guarantees provided by such systems. On the other hand security objectives also need to be provided with high availability requirements and strong threat models. In this context, another important challenge is data availability. Yet new mechanisms are required to guarantee the availability of the data itself. As compared to Estonia's government use of blockchain technology in support of governmental services, other governments are still at an early, largely conceptual stage of planning. Most benefits of the technology in these countries still relate to potentially increased transparency and more efficient workflows.

7. References

[1] M. Niranjanamurthy, B. N. Nithya, S. Jagannatha, "Analysis of Blockchain technology: pros cons and SWOT", *Cluster Computing*, pp.

[2] Professor Ivan Martinovic, Blockchains: Design Principles, Applications, and Case Studies ,Develop the future of E governance

[3] Blockchains for Governmental Services: Design Principles, Applications, and Case Studies December Center for technology and Global Affairs, www.clga.ox.ac.uk 2017

[4] Case Study Dubai - The first City on the blockchain smartdubai.ae january 2017

[5] The Blockchain (R)evolution – The Swiss Perspective White Paper February 2017

[6] Abeyratne, S. A., & Monfared, R. P. (2016). Blockchain ready manufacturing supply chain using distributed ledger. Loughborough University.

[7] Distributed Ledger Technology: beyond block chain A report by the UK Government Chief Scientific Adviser Jan 19, 2016

[8] "Nasdaq's Blockchain Technology to Transform the Republic of Estonia E-Residency Shareholder Participation,"Nasdaq Press Release,February16,2016

[9] Badzar, A. (2016). Blockchain for securing sustainable transport contracts and supply chain transparency- An explorative study of blockchain technology in logistics. Lund University.

[10] Rizzo, P. (2016). World's Largest Mining Company to Use Blockchain for Supply Chain. CoinDesk. Available at http://www.coindesk.com/bhp-billiton-blockchain-mining-company- supply-chain/

[11] Condos, J., Sorrell W. H., and Donegan S. L. (2016). Blockchain technology: Opportunities and Risks. VERMONT.

[12] Benjamin S. Buckland, Fred Schreier, Theodor H. Winkler, democratic governance challenges of cyber security, DCAF HORIZON 2015 WORKING PAPER No. 1

[13] Brodbeck, L. (2015). Blockchain Could Help Fight Corruption In Honduras. Benzinga. Available from: https://www.benzinga.com/news/15/05/5518234/blockchain-could-help-fight-corruption-in-honduras

[14] Kibum Kim, Consultant at KPMG, Taewon Kang, Ph.D Candidate at Seoul National University, Seoul, Korea, The Potential Risks and Challenges of the Blockchain Technology

[15] Blockchain Technology: Possibilities for the U.S. Postal Service, Report Number RARC-WP-16-011