Review of Various Block-chain Based SSL Techniques

P. Rajitha Nair[1], Dr. Ramya Dorai[2], Vinod Unnikrishnan[3]

[1] *Computer Science Department, NHCE, Bengaluru, Karnataka, India*
[2] *Computer Science Department, TJIT, Bengaluru, Karnataka, India*
[3] *Virtusa, Bengaluru, Karnataka, India*

***Abstract* - Operating under constant threat of attacks, users have long been accustomed to verify the SSL certificate, to ensure that the site is secure. SSL is used to transmit sensitive information over the Internet, and it has been a significant driver of e-commerce from long. This process involves protocols including the Secure Sockets Layer (SSL) and Transport Layer Security (TLS), as well as certificate authorities (CAs), entities that issue digital certificates to organizations or individuals. The research topic being pursued is an alternative approach to ensure trust can be established using certificates – via the Block-chain algorithm**

***Keywords* – SSL, TLS, Block-chain, Proof Of Concept, Proof Of Work**

I. INTRODUCTION

Public Key Infrastructure

Public Key Infrastructure (PKI) is a collection of roles, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption. PKI facilitates secure transfer of information for various network activities such as e-commerce, internet banking and confidential email. It is necessary where passwords are inadequate authentication method and rigorous proof is required to confirm the identity of the parties involved in the communication and to validate the information being transferred.

In cryptography, PKI is an arrangement that binds public keys with respective identities of entities (like people, companies, educational institutions). This binding is established via process of registration and issuance of certificates at and by a certificate authority (CA). This may be carried out by an automated process or under human supervision, depending on the assurance level of the binding,

The main actors in PKI are:

- Registration Authority (RA) - RA's function is accepting requests for digital certificates and authenticating the entity making the request
- Certifying Authority (CA) –CA's function is to ensure that an entity is uniquely identifiable within their domain on the basis of entity's information
- Validation Authority (VA) – VA's function is to provide this entity's information on behalf of the CA.

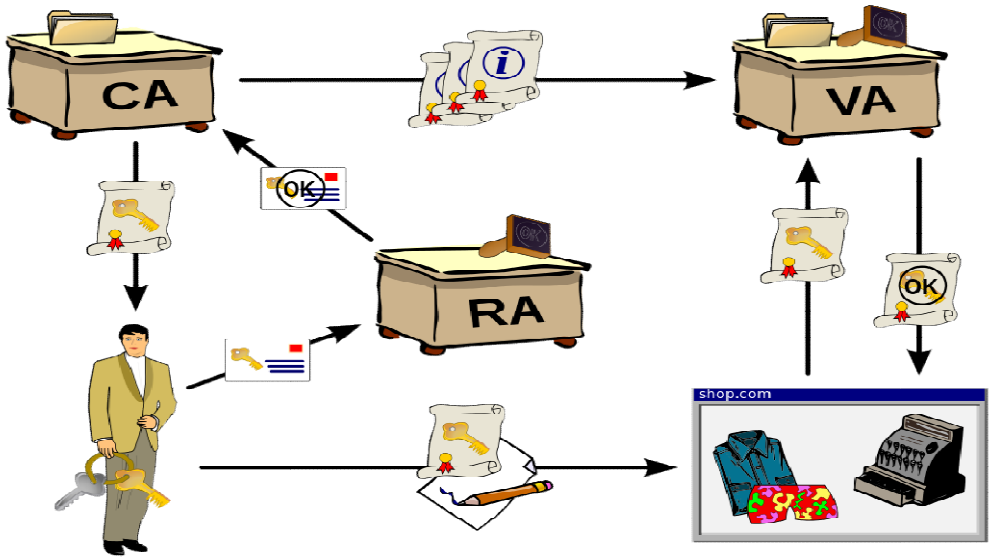

Figure 1: Public Key Infrastructure

Public Key Certificate

A public key certificate, referred as digital certificate or identity certificate, is an electronic document used to prove the ownership of a public key. The certificate has the key's information, owner's identity information, and the Certificate Issuer's digital signature that has verified the certificate's contents. If the signature is valid, and the software examining the certificate trusts the issuer, then it can use that key to communicate securely with the certificate's owner. In email encryption, code signing, and e-signature systems, a certificate's owner is usually a person or organization. However, in Transport Layer Security (TLS) a certificate's owner is typically a computer or other device, though TLS certificates may identify organizations or individuals in addition to their core role in identifying devices. TLS (Secure Sockets Layer - SSL) is a protocol for safely and securely access web and is a part of HTTPS.

In PKI, the CA issues the certificate and charges customers for these certificates. In a web of trust scheme, individuals sign each other's keys directly, in a format that performs a similar function to a public key certificate.

X.509 is a widely used format for these certificates. X.509 is a generic implementation and hence usually constrained by profiles defined for specific use cases, e.g.: RFC5280.

II. BLOCK-CHAIN TECHNOLOGY

A block-chain is a continuously growing list of records (blocks) linked and secured using cryptography. Each block usually has a hash pointer as a link to a preceding block, a timestamp and transaction data. Data is not modifiable in block chain. For use as a distributed ledger, a block-chain is typically managed by a peer-to-peer network collectively adhering to a protocol for validating new blocks. Network majority is required to alter data in a given block as altering in one block requires data to be altered in all subsequent blocks.

Block-chains are secure by design and are an example of a distributed computing system with high Byzantine fault tolerance. Decentralized consensus has therefore been achieved with a block-chain. This makes block-chains potentially suitable for the recording of events, medical records and other records management activities, such as identity management, transaction processing, documenting provenance, or food traceability.

The first distributed block-chain was conceptualized by an anonymous person or group known as Satoshi Nakamoto, in 2008 and implemented the following year as a core component of his digital currency – bitcoin – where it serves as the public ledger for all transactions. The invention of the block-chain for bitcoin made it the first digital currency to solve the double spending problem without the use of a trusted authority or central server.

By storing data across its network, the block-chain eliminates the risks that come with data being held centrally. The decentralized block-chain may use ad-hoc message passing and distributed networking. The network is devoid of central vulnerable points or point of failure. Block-chain security methods include the use of public-key cryptography. A public key (a long, random-looking string of numbers) is an address on the block-chain withvalue tokens sent across the network recorded as part of that address. A private key is like a password that gives its owner access to their digital assets or otherwise interact with the various capabilities that block-chains now support. Data stored on the block-chain is generally considered incorruptible. Block-chain database consists of two types of records - transactions and blocks. Valid, hashed and encoded transactions in a Merkle tree format form the Blocks.Every block has the hash of the prior block in the block-chain hence linking the two blocks.

Merkle Tree

In cryptography a hash tree or Merkle tree is a tree in which every leaf node is labelled with a data block and every non-leaf node is labelled with the cryptographic hash of the labels of its child nodes. Efficient and secure verification of contents of large data structures are allowed by Hash trees which is a generic form of hash chains and lists.

Computing a number of hashes is required to ascertain that a given binary hash tree has the leaf node. The number of hashes is a function of the logarithm of the number of leaf nodes of the tree. In comparison hash lists function is proportional to the number of leaf nodes itself.

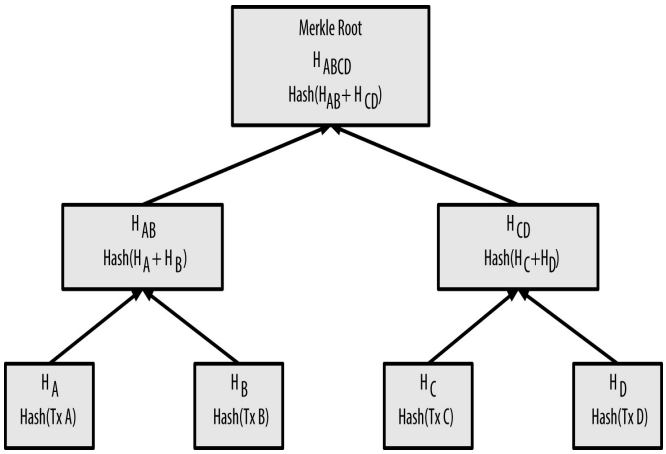

Figure 2: Merkle Tree

There are two major ways in which Block-chain can be implemented algorithmically and Distributed Consensus arrived at – Proof of Work and Proof of Stake.

III. PROOF OF WORK

Proof-of-work (PoW) algorithm requires participants to solve complicated cryptographical puzzles in order to validate transactions and create new blocks. With each solved puzzle there is a new block created and the reward is thus the block that is created.

IV. PROOF OF STAKE

Proof-of-stake (PoS) is a type of algorithm the blocks are usually said to be forged or minted, rather than mined. Also, usually all the blocks are created in the beginning and the total number of blocks usually never changes afterwards. Hence transaction fees are the only rewards for forgers in PoS.

REFERENCES

[1]. F. Imbault, M. Swiatek, R. de Beaufort, R. Plana 'The green blockchain Managing decentralized energy production and consumption', IEEE 2017

[2]. PwC, 'Blockchain and smart contract automation: How smart contracts automate digital business', 2016

[3]. Kamanashis Biswas, VallipuramMuthukkumarasamy, 'Securing Smart Cities Using Blockchain Technology' 2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems, 2016

[4]. KonstantinosChristidis, Michael Devetsikiotis,'Blockchains and Smart Contracts for the Internet of Things' IEEE. VOLUME 4, 2016

[5]. Chad Brubaker, Suman Jana, Baishakhi Ray, SarfrazKhurshid,VitalyShmatikov 'Using Frankencerts for Automated AdversarialTesting of Certificate Validation in SSL/TLS Implementations' 2014 IEEE Symposium on Security and Privacy

[6]. M. Ali, J. Nelson, R. Shea, and M. J. Freedman, 'Blockstack: A global naming and storage system secured by blockchains,' in USENIX Annual Technical Conference (ATC), June 2016

[7]. J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, 'SoK: Research perspectives and challenges for Bitcoin andcryptocurrencies,' in IEEE Symposium on Security and Privacy (S&P), May 2015

[8]. Feiyan Mu Jiafen Zhang and Jing Du, Jie Lin 'Application of the Secure Transport SSL Protocol in Network Communication' Fourth International Symposium on Computational Intelligence and Design, 2011

[9]. Guy Zyskind, Oz Nathan, and Alex Pentland, 'Enigma: Decentralized Computation Platform with Guaranteed Privacy.' 2015

[10]. LoiLuu, Viswesh Narayanan, KunalBaweja, ChaodongZheng, Seth Gilbert, and PrateekSaxena, 'Scp: A computationally-scalable byzantine consensus protocol for blockchains', 2015