Towards Creating Public Key Authentication for IoT Blockchain

Deepa Pavithran
Abu Dhabi Polytechnic,
Abu Dhabi, United Arab Emirates
deepa.pavithran@adpoly.ac.ae

Khaled Shaalan
The British University in Dubai,
Dubai, United Arab Emirates
khaled.shaalan@buid.ac.ae

Abstract— **Besides confidentiality and privacy, trust is an important factor for any IoT system. When a sensor send data that is signed with its private key, the receiving nodes verify it using the public key of the sensor. Hence, it is understood that authenticating the public key of the system is part of creating trust within the system. Traditionally, trust is maintained using Public Key Infrastructure (PKI) where a centralized Certificate Authority (CA) is used for authenticating the public keys. However, a centralized system can result in single point of failure where CA can be compromised or can act maliciously. Decentralizing this system using blockchain and by automating the process of certificate authentication without the need for a central third party can overcome the above-mentioned limitations. We identify the challenges in creating such a system and propose a generic framework for PKI in IoT infrastructure using blockchain that can provide the functions of a CA.**

Keywords—blockchain, Public Key Infrastructure, Internet of Things, decentralized, trust

I. INTRODUCTION

Internet of Things is a promising technology with millions of intelligent devices collaborating with each other to create a smart world. They can sense information from physical environment, communicate within different devices and can take appropriate decisions. It generally consist of five components (1) sensors to collect information from surroundings, (2) Actuators to trigger a device for particular functions, (3) Computing node that process the information sensed by the sensor (4) Receiver to receive message from other devices and (5) Communicator to pass message to other devices [1].

In a network of IoT devices that communicate with each other, before sending any data, the receiving device should be authenticated within the network. This authentication can be effectively done by providing certificates to the devices. However the traditional certification process includes a centralized Certificate Authority (CA) to generate and issue the certificate. A major drawback of this approach is that the certificates are issued by a third party which could lead to single point of failure within the system, where the third party could potentially act maliciously or can be compromised. According to a recent report, thousands of malware samples uploaded to VirusTotal was given valid certificates by a well-known Certificate Authority [2]. Another major weakness of this centralized approach is the cost and complexity of deployment. The complexity of a possible solution and intense computations of asymmetric cryptography makes it less suitable for IoT devices. In addition, dedicated team of experts are required to handle such PKI implementation.

Blockchain enables all devices to communicate each other and automatically verify the transactions generated by the devices. In case of IoT, the data is sensitive and should be protected. Hence when a transaction is carried out, the device should verify to whom it is sending the data. A centralized management and a trusted authority entirely contradicts with the concept of blockchain which is basically a decentralized, transparent solution that provides trust through cryptographic techniques. Compared with the conventional PKI, blockchain based PKI have the advantage of eliminating single point of failure, provides certificate transparency and reliable transaction record. It can prevent man in the middle attack and minimize the control of third parties on users keys. Although the concept of blockchain originated as a tool for cryptocurrency, the concept can also be utilized for other applications including IoT [3]. Several modifications of the traditional bitcoin protocol are available in literature for IoT. But it is understood that the challenges faced in IoT-blockchain usecases differ from the cryptocurrency usecases.

Asymmetric encryption uses public and private key. Private key is kept secret within the device while, public key is made public. Even though the public key is public, it should be distributed in a trusted manner otherwise a phishing attack can lure the devices to use the public key of an attacker and will result in sending confidential data to the attacker.

In this paper we use all the advantages of blockchain technology to create a framework for public key authentication system for IoT devices. We assume, the device has the capability to perform basic cryptographic functions and the private keys are stored as hardware embedded cryptographic chips attached to the device.

The rest of the paper is organized as below. We provide a brief background on Public key infrastructure and blockchain in Section II. Related works are listed in Section III. Section IV highlights the challenges in replacing a centralized PKI system to a decentralized system. Section V elaborates the proposed framework and Section VI provides implementation details and comparison of the traditional approach to our approach. Finally, Conclusion and future work is provided in Section VII.

II. BACKGROUND

A. Public key infrastructure

Public key Infrastructure is used as an underlying technology to support confidentiality, integrity, authentication and non-repudiation. It manages the digital certificates and encryption keys of a given identity in a permanent and reliable way. Currently the most commonly used approach for PKI is the CA based PKI. The CA based PKI is centralized which includes a trusted third party and hence has the disadvantage of single point of failure. Apart

978-1-7281-5061-1/19/$31.00 ©2019 IEEE

from the CA based model, The Web of Trust Model is a decentralized PKI, where public keys are signed by trustworthy users. This concept is used in PGP [4]. However, it is less popular due to the fact that, a new user will have to meet someone in person to verify its identity and get its public key signed.

The three core functional components to a PKI are certificate authority, repository and management function [5]. A Certificate Authority is a trusted third Party that issues certificates, Repository is an LDAP Enabled Directory Services to store keys, certificates and certificate revocation list(CRL). Management Functions are set of policies and procedures that are typically implemented. In addition to the core functions, additional components of PKI are Key recovery service and Registration Authority (RA). Key recovery service provides automated key recovery in case of lost or stolen keys and Registration Authority services includes collecting user information, verifying user identity, register the user according to policies and accept certificate requests. Systems performing CA and RA series are often referred to as certificate servers and registration servers. The core functions of a PKI are issuing certificates, revoking certificates, storing and retrieving certificates. In a traditional PKI, the keys can be generated by the client or the other option is CA generating for the client. This depends on the application for which the key will be used. If key is used only for signing purpose, then it is better that the key is generated by the client itself. In case if the key is used for decryption purpose to provide confidentiality of the message, then it might be prudent to have the CA generate or have access to the key [6]. This is to ensure if client loses the keys the encrypted information can still be decrypted. After generating the key, client provides a copy of the public key to the CA to certify. To verify the identity of the user and to ensure it is a legitimate user, Registration Authority is used. The functions of RA and CA can be combined and the generated certificates are stored in a certificate directory. Users can look up the directory for validity of the certificates. Figure 1, illustrates the steps of PKI. Suppose Bob wants to send a message to Alice using her public key. Alice should initially generate public-private key pair and submit the public key along with her identity to RA. It verifies the identity and request for certificate to CA. A certificate is basically, signing the public key of the user with the private key of the CA. CA issues and stores the certificate in the directory. Alice can get a copy of the certificate from CA. When Bob wants to encrypt a message, he checks the directory for Alice's Certificate and in turn verifies the signature of CA and the respective validity of the certificate.

B. Blockchain

Blockchain is basically a distributed ledger, where a collection of data is shared and synchronized among different nodes in the network that are geographically spread through distinct locations [7]. It consists of a growing list of records, called blocks that are linked together using cryptography. The concept of blockchain was introduced with bitcoin, which is a decentralized payment system that eliminates the need of central authority and provides solution to double spending problem. Each block in the blockchain is linked to its previous block using hash functions making it tamper proof ledger of records. The first block is called the genesis block. Transactions or records are stored in each block. Generally, each block contains hash of previous block, timestamp and transactions. In the bitcoin blockchain, the validation of the transactions is done by a group of miners who compete to solve cryptographic puzzle in order to get reward as bitcoins. This process is called Proof of Work (PoW). However, bitcoin mining consumes a good portion of the world's energy. This is due to the fact that mining involves calculation of trillions of hashes per second[8] which is continuously increasing per year. Such kind of validation methods are not suitable for IoT devices which are resource constrained. There are several alternatives for PoW in IoT. An example is IOTA, a decentralized protocol typically for IoT which uses Tangle consensus [9].

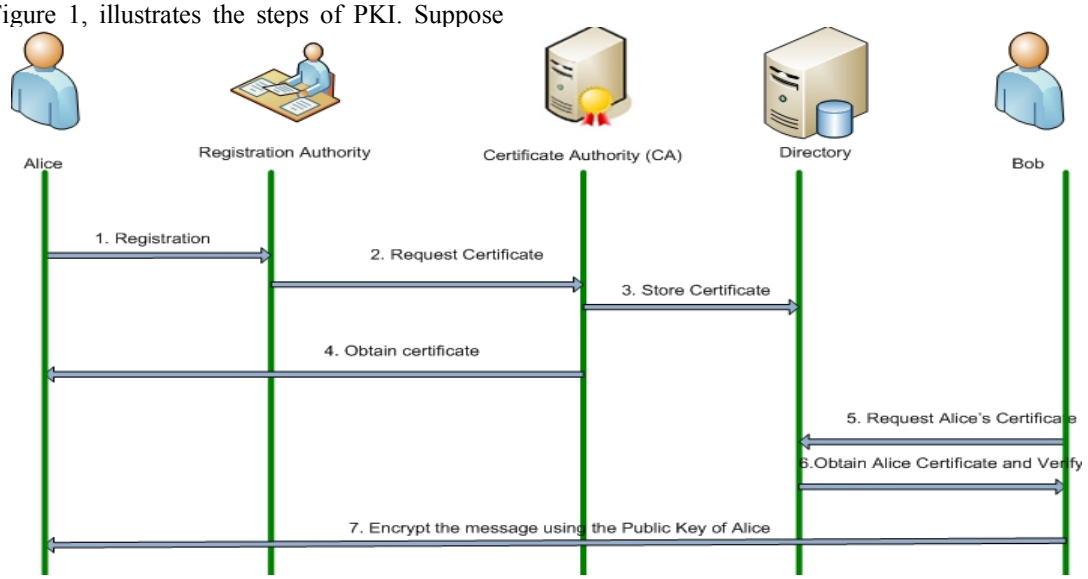

Fig:1 CA based Public Key Infrastructure

III. Related Work

PKI using blockchain was proposed in several prior works. Blockstack [10] is blockchain based naming and storage system. It enable users to register unique, human-readable usernames and its public-keys along with additional data. Blockstack ID is PKI and identity system based on Namecoin. Namecoin [11] is a cryptocurrency which is a fork of bitcoin and offers the same features as bitcoin with the addition of a name/value store that can be used to hold arbitrary data. It uses PoW. The main motivation for starting Namecoin was to decentralize DNS using blockchain technology.

Emercoin [12] is a blockchain based PKI which uses a hybrid system by combining PoW and Proof of Stake consensus. However several limitation of this approach was identified in [13]. Certcoin [14] is a decentralized PKI system based on bitcoin. Axon and Goldsmith [15] propose Blockchain based PKI that provides privacy. Certchain [16] design a certificate management system based on four layer blockchain architecture. It uses a rank based consensus protocol. But this is mainly for SSL/TLS connections and is not applicable for IoT. Blockchain based system to secure messages is proposed by Khacef and Pujolle [17]. It uses smart contract to verify the identities and its public keys and validates user certificates. It is not based on Namecoin and they use their own system but it provides only registration and does not provide key recovery or key updates. In Yakubov et al. [13], authors adds blockchain features to extensions field of X509V3 digital certificates to make it a hybrid certificate.

However all the above approaches are for providing certificates for SSL/TLS for domain names and servers. These approaches cannot be directly applied for IoT, as IoT architecture and operations differ from these. Blockchain based PKI for crowdsources IoT sensor information is proposed in Pinto et al. [7]. Their approach is based on keybase and revocation and updating of keys in key base is a trivial task is not identified.

IV. Challenges

Some of the challenges in creating PKI for IoT blockchain are as follows

Private key Storage: In a bitcoin blockchain, private keys are stored with the users in their wallet. If the wallet is lost all bitcoins are lost. However in case of IoT, private keys should be secured by either embedding it in the hardware or through softwares. Cryptographic keys can be stored securely in chips which provide physical and electronic security mechanisms. Hardware embedded cryptographic chips are available that can store the private key and can also perform the required mathematical operations.

Scaling PKI for Billions of Devices: IoT devices are mostly deployed in public. Grouping and managing certificates for billions of devices is a key challenge. Only authorized devices should be provided access to the network.

Heterogeneity of the devices: Devices are manufactured by different manufactures without specific standards. Hence bringing all these devices under a common rule is a challenge today.

Storage: Blockchain is a growing ledger where data is stored in a distributed fashion. Distributing the data within light node is impractical in the long run. Hence the storage should be designed within edge nodes or separate cloud storage should be used.

Consensus: Bitcoin blockchain performs expensive consensus mechanism which consume a good portion of energy. However for a resource constrained IoT, this is impractical. Hence designing an energy efficient consensus is a challenge.

V. Proposed Approach

Our approach is to create a blockchain including edge nodes and IoT devices, where each edge nodes are not resource constrained devices and is located in different geographic locations, and connected to IoT devices within the location.

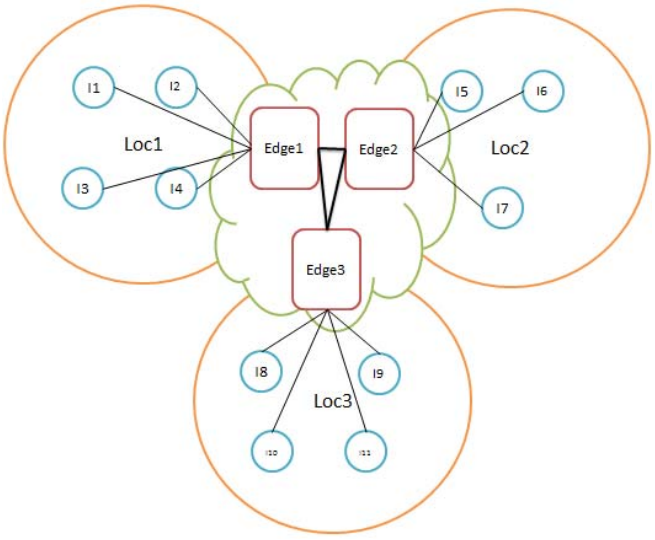

Fig: 2 Device connectivity with edge nodes

Fig: 2, is a generic figure illustrating the devices in various locations and its connectivity to the edge nodes. Different locations are identified as {loc1,loc2,…loc_n}, edge node as {Edge1,Edge2…$Edge_n$} and IoT device as {I1,I2,I3…I_n} Fig: 3 provides the block structure and the representation of data to be added in the blockchain. Each block contain block header, hash of previous block, Merkle root and transactions. Transactions include Device ID, Public key of the device, certificate, location of device, time stamp and expiry data. The detailed process is illustrated in Fig: 4.

Initialization:

1. IoT devices are grouped based on the locations where each device is registered to an edge node that are not resource constrained devices.

2. Private keys of each IoT device are embedded within the device and the device is capable of performing cryptographic operations.

3. Edge nodes generate their own private/public key pair and their certificates are validated through Web of Trust model. These transactions are initially added to the blockchain and distributed to all the nodes.

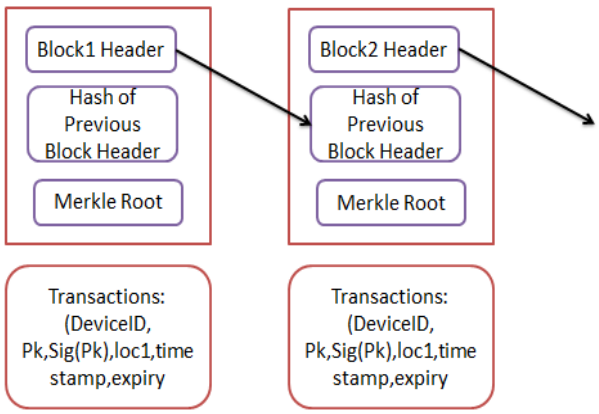

Fig:3 Block Structure of the proposed approach

Registration:

1. When a new IoT device is added to the network, the device is registered to its edge-node with its Device ID, Public key and timestamp

Blockchain process:

1. Edge node create transaction

Device ID, Pk, Sig(Pk), loc1 and share the transaction with its neighboring nodes

2. The neighboring nodes elected through a cluster head selection process validate the transaction and adds the same to the blockchain

3. The validated transactions are created as blocks and added to the blockchain, which is distributed among all the edge nodes. When an IoT device in loc_i tries to establish a communication with a device in loc_j; it contacts its edge node, which would in turn verify the device's public key signed by corresponding edge-node based on the latest transactions.

Key Revocation/Key updates:

1. When a device private key is compromised, the new key can be registered to the edge node, which follows the same steps as above. Only the latest transactions for the device will be used and hence the older key will automatically become invalid.

2. When the private key of an edge node is compromised, it will have to create new transactions for all the devices within its network.

VI. Implementation and Comparison

RaspberryPi with a sensor can be used to simulate the IoT. We implemented the blockchain process on two edge nodes. We used Ubuntu 16.04 LTS and Geth was used to run a full Ethereum node implemented in GO[18]. We used solidity, to program the smart contract and deployed it in the network. Smart contract store device_ID and public key of IoT in the blockchain. A screenshot of the Ethereum wallet executing smart contract is shown in Fig:5.

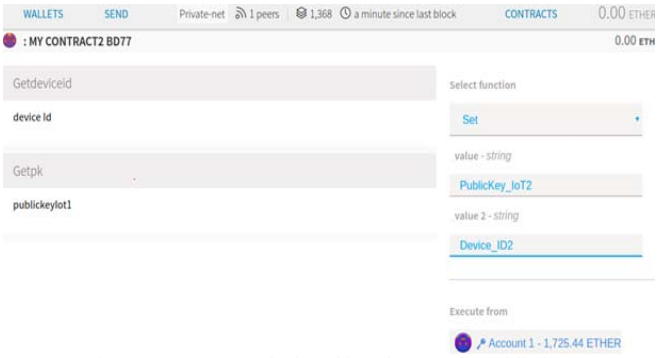

Fig:5 Smart contract deployed in Ethereum for public key

A comparison of our approach with the functions of traditional CA based PKI is given in Table1.

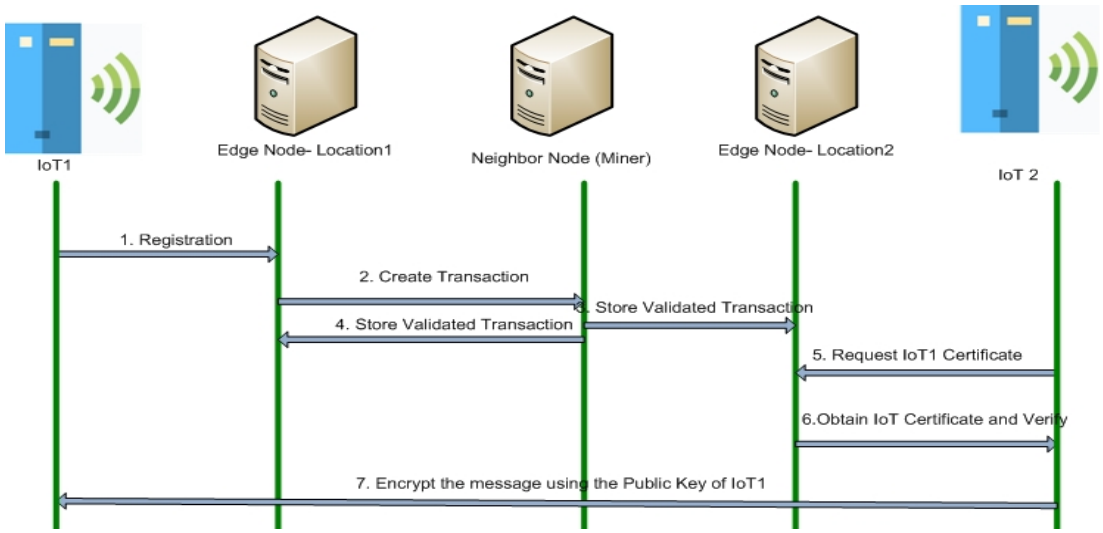

Fig: 4 Steps in the blockchainchain based public key authentication

Table1: Comparison of CA based PKI with Blockchain based PKI for IoT

PKI Functions	CA Based PKI	Blockchain Based PKI for IoT (This Paper)
Issuing Certificates	CA sign and stamp the certificate after authenticating the identity of the requestor. The certificate may be returned back to the owner or posted in a repository.	Edge node within the network sign and stamp the identity of the IoT device. It create transaction that is shared to other edge nodes for validation and then added to blockchain
Revoking Certificates	CA revoke the certificate before its expiry in case of lost or stolen private keys. The revoked certificates will be included in the Certificate revocation list (CRL)	The new key can be registered to the network. As only the latest transactions for the device will be used, the older key will automatically become invalid
Storing and Retrieving Certificates	Certificates are stored via directory services	Certificates are stored as distributed data structure
Updating Keys	Certificates have a validity of usually one year or two. After the expiry of the key, Keys are updated to new key	After the expiry of the key, Keys are updated to new key
Backing up Keys	Keys should be backed up in case if user forgets the password or in case of a virus attack	Private keys are embedded within the IoT device Hardware

VII. Conclusions and Future Work

Blockchain is a promising technology that can provide trust among 'things' without the need for a central authority. We provide a framework for managing public keys of IoT devices in a decentralized way. Our approach use edge nodes for verifying and validating the transactions. We identify the challenges and provide comparison of the CA based PKI functions with the Blockchain based PKI for IoT. However we have not considered the confidentiality of the data between the IoT and the edge node, which could be considered as future work.

References

[1] S. Horrow and A. Sardana, "Identity management framework for cloud based internet of things," InProceedings of the First International Conference on Security of Internet of Things, ACM pp. 200–203, 2013.

[2] F.Y. Rashid, "Attackers are signing Malware with valid certificates," Duo Security, [Online]. Available: https://duo.com/decipher/attackers-are-signing-malware-with-valid-certificates, 2019[Accessed: 12-Sep-2019].

[3] R. Dorri, Ali and Kanhere, Salil S and Jurdak, "Towards an Optimized BlockChain for IoT Ali," Proc. Second Int. Conf. Internet-of-Things Des. Implement., pp. 173--178, 2017.

[4] S. Garfinkel, PGP: pretty good privacy. O'Reilly Media, Inc., 1995.

[5] RSA Data Security, "Understanding Public Key Infrastructure (PKI)," White paper, RSA, pp. 1–7, 1999.

[6] G. P. Kenneth G Paterson, "A comparison between traditional Public Key Infrastructures and Identity-Based Cryptography," Inf. Secur. Tech. Rep. 8, vol. 3, pp. 57–72, 2003.

[7] G. Pinto, J. P. Dias, and H. S. Ferreira, "Blockchain-based PKI for Crowdsourced IoT Sensor Information," International Conference on Soft Computing and Pattern Recognition, Springer, Cham, pp. 1–16, 2018.

[8] "www.blockchain.com/charts/hash-rate," blockchain.com, 2019. [Online]. Available: https://www.blockchain.com/charts/hash-rate.

[9] S. Popov, "IOTA whitepaper v1.4.3," pp. 1–28, 2018.

[10] M. Ali, J. Nelson, R. Shea, and M. J. Freedman, "Blockstack : A Global Naming and Storage System Secured by Blockchains," USENIX Annu. Tech. Conf., pp. 181–194, 2016.

[11] H. Kalodner, M. Carlsten, P. Ellenbogen, J. Bonneau, and A. Narayanan, "An empirical study of Namecoin and lessons for decentralized namespace design," WEIS, 2015.

[12] O. Konashevych, "Emercoin Blockchain Anchoring as a Way of Singing Contracts," TERECOM@ JURIX (pp. 17-29), 2018.

[13] A. Yakubov, W. M. Shbair, A. Wallbom, D. Sanda, and R. State, "A blockchain-based PKI management framework," IEEE/IFIP Netw. Oper. Manag. Symp. Cogn. Manag. a Cyber World, NOMS 2018, pp. 1–6, 2018.

[14] C. Fromknecht, D. Velicanu, and S. Yakoubov, "CertCoin: A NameCoin Based Decentralized Authentication System," pp. 1–19, 2014.

[15] L. Axon and M. Goldsmith, "PB-PKI : a Privacy-Aware Blockchain-Based PKI Conventional Approaches to PKI," Proc. 14th Int. Jt. Conf. E-bus. Telecommun. (ICETE 2017), pp. 311--318, 2017.

[16] J. Chen, S. Yao, Q. Yuan, K. He, S. Ji, and R. Du, "CertChain: Public and Efficient Certificate Audit Based on Blockchain for TLS Connections," Proc. - IEEE INFOCOM, vol. 2018–April, pp. 2060–2068, 2018.

[17] K. Khacef, G. Pujolle,"Secure Peer-to-Peer communication based on Blockchain", Workshops of the International Conference on Advanced Information Networking and Applications (pp. 662-672). Springer, Cham, 2019.

[18] "Official Go implementation of the Ethereum protocol," *Github*, 2019. [Online]. Available: https://github.com/ethereum/go-ethereum. [Accessed: 12-Sep-2019].