KICS The Korean Institute of Communications and Information Sciences

Available online at www.sciencedirect.com

ScienceDirect

ICT Express xxx (xxxx) xxx

www.elsevier.com/locate/icte

Key management for blockchain technology

Om Pal[a,*], Bashir Alam[b], Vinay Thakur[a], Surendra Singh[a]

[a] *Ministry of Electronics and Information Technology, 6, CGO Complex, New Delhi, 110003, India*
[b] *Department of Computer Engineering, Jamia Millia Islamia, Jamia Nagar, New Delhi, 110025, India*

Received 8 June 2019; accepted 11 August 2019
Available online xxxx

Abstract

Public Key Infrastructure (PKI) is used in Blockchain Technology to authenticate the entities and to ensure the integrity of the blockchain. Proper Protection of Bitcoin wallet is required for private keys, seeds and keys stored in external hardware in Blockchain infrastructure. In this paper, overview of Blockchain, analysis of existing PKI for Blockchain and key management for Blockchain wallet are discussed. To achieve the confidentiality of sensitive records over the Blockchain network, a Group Key Management scheme for secure group communication is also proposed.

Keywords: Blockchain; Bitcoin; Wallet key; Key management; Blockchain key management; Blockchain group key management

1. Introduction

Blockchain Technology or decentralized secure ledger is one of the most popular technology which has the capability to eliminate the requirement of third party to validate the transactions over the Peer-to-Peer network. Using the consensus of the existing members of the network, transactions over the network are validated. In Blockchain Technology, members of the network keep the transactions' data in form of ledger and this ledger is updated by adding of new block of transactions to maintain the integrity of the data.

In year 2009, Satoshi Nakamoto proposed the Blockchain based digital currency called Bitcoin. In this Bitcoin digital currency, transactions are allowed among the peers to manage the currency. The major advantage of this digital virtual currency (Bitcoin) is that there is no need of central authority to authenticate, control or validate the transactions.

Blockchain Technology is under developing phase. However, this technology has shown the potential to transform the existing business process, e-Governance services, financial services, health care services, agriculture services etc. into new dimensions where additional advantages in term of efficiency, cost, trust etc. are guaranteed [1–10]. Blockchain Technology is useful in many areas which include — e-Tender through Blockchain, Blockchain for IoT Devices, Blockchain for banking, Blockchain for Insurance claim settlement, Blockchain for Taxation etc.

The data structure of the Blockchain is a structured list of blocks. Blocks are connected in form of list whereas current block stores some values in its header like hash of previous block, Blockchain address of the previous block etc.

Each block consists two parts: header and body. The header comprises block number, hash value of previous block to maintain the integrity of the Chain, hash of body of current block to maintain the integrity of the transaction data, time stamp, nonce, Blockchain address of block creator and other desired information. Body of the block contains one or more transactions. (See Fig. 1.)

In Blockchain, data is stored in a decentralized manner over the network and a copy of each transaction along with hash of transaction data is stored in a form of ledger with each member of the network. In decentralized storage, for any intruder it is tough to alter the stored data at majority places. Therefore, decentralized storage provides higher cryptographic security compared to centralized storage.

Approval of transactions is given by the majority of the peer members. Therefore, this technology completely eliminates the role of central approving authority. Due to decentralized approval of the transaction, hacking is difficult, transactions are automatically approved through consensus protocols and

* Corresponding author.
E-mail address: ompal.cdac@gmail.com (O. Pal).

Peer review under responsibility of The Korean Institute of Communications and Information Sciences (KICS).

https://doi.org/10.1016/j.icte.2019.08.002

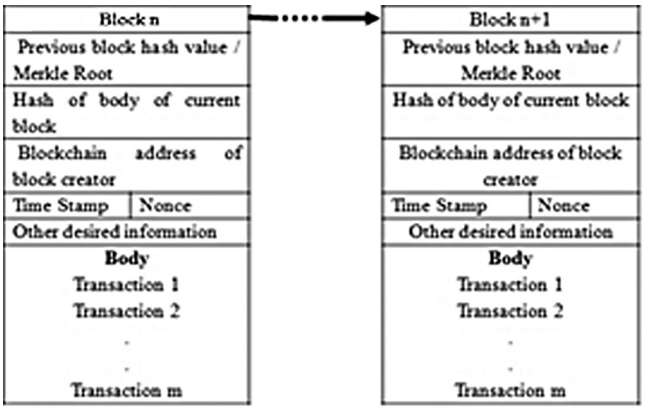

Fig. 1. Block structure.

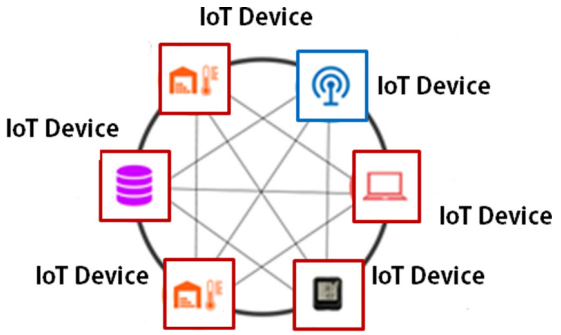

Fig. 2. IoT network.

security expenses are also saved. In Blockchain, data is quick verifiable, security and privacy is preserved and no alteration is possible without consensus of the majority. By using smart contract promptness of the transaction is also assured.

Blockchain Technology is not a replacement of the Public Key Infrastructure (PKI) but this technology uses the PKI to identify and authenticate the members to participate in the Blockchain network. For managing the PKI infrastructure of Blockchain, many authors proposed the possible solutions [11–15]. In Blockchain Technology, there is also a challenge to manage the massive amount of cryptographic keys for Bitcoin wallets. To manage the Bitcoin wallet keys, authors presented various solutions [16–23].

Blockchain for IoT Systems Due to interconnection of IoT devices over the internet, there is a high chance of security breach in the IoT system. If IoT systems are not well protected then such systems can be attacked easily. Researchers are continuously exploring the possible threats for such systems and they are inventing new technologies, models, frameworks to counter the possible threats. IoT system accommodates a huge amount of data, multiple heterogeneous devices, human community interaction, supply chain partners etc. Due to heterogeneous connectivity, there is more space for hackers to breach the security of the system. For example, due to connectivity of critical systems such as power plant, gas plant, health care units with internet, there is a need to assure the security of such IoT systems in efficient way. There should be proper integrity check, authentication, confidentiality of data, consensus of network members to restrict the entry of false station, prevention from one point of failure, agreement of majority on critical commands, denial of service attack, elimination of other various attacks such as replay attack, man-in-middle, side channel attack etc. through advanced technologies such as Blockchain Technology. (See Fig. 2.)

Blockchain ensures the distributed authentication and trust among the peer nodes of the IoT system and as a result, it means an additional security layer for the IoT system. Distributed architecture of Blockchain can help IoT system in many ways like-

- Proper tracking of sensor data using Blockchain: With consensus of majority, it prevents the wrong measurement of sensor data and the replacement of true value of measurement with false values.
- Using Blockchain Technology, IoT sensors can exchange the data without involving the third party for establishment of trust. Blockchain platform provides the distributed trust environment for sharing the data.
- Cost of the operation and deployment of IoT systems can be reduced due to non-requirement of intermediary as it supports the peer-to-peer communication.
- In case of any mismatch of the data, faulty IoT devices can be easily detectable with help of hashing mechanism of Blockchain Technology.
- By incorporating the Blockchain Technology in IoT systems, a simplified business process with low operational cost and with higher efficiency can be emerged.

Rest of the paper is organized as follows: in Section 2, we analyzed the key management for Blockchain infrastructure. In Section 3, Group Key Management for Blockchain Network is proposed. In Section 4, conclusion is given and at the end, the list of references is given.

2. Key management for blockchain

Efficient and secure key management is a challenge for any cryptographic system. If intruder is able to discover the keys by any mechanism like bruit force, side channel attack, physical access of system, weak encryption, replay attack etc. then intruder is able to steal everything from the targeted system. Therefore, management of keys is one of the most critical component of the cryptographic system. No infrastructure is secure if its keys are not secure. Blockchain infrastructure uses PKI to authenticate the IoT devices and security of the infrastructure is dependent on the trustiness of third party. In this section, key management for Bitcoin wallet and PKI for Blockchain are discussed.

2.1. Key Management for Bitcoin Wallet

Bitcoin Wallet is similar to the bank account where Bitcoin currency is kept. To use the Bitcoin currency from the Bitcoin Wallet, the owner of the Wallet accesses the Wallet currency

Please cite this article as: O. Pal, B. Alam, V. Thakur et al., Key management for blockchain technology, ICT Express (2019), https://doi.org/10.1016/j.icte.2019.08.002.

by using its private key. When user uses its private key then corresponding account is accessible to the owner for accessing the digital currency. Once owner has the access of its Bitcoin currency he/she may spent it.

Overall security of the Bitcoin Wallet depends on, how anyone can keep its private key secure. If private key of the Wallet is compromised by any means like physical theft of the storing device, side channel attack or hacking then hacker can steal the Bitcoin currency easily. Therefore, it is advisable to manage the keys for Bitcoin wallet efficiently. There are various Bitcoin Key Management approaches; some of them are given below.

Local Key Storage In this Key management approach, private keys are stored in the local storage of the device and these keys are accessible by the Bitcoin software from the specified location like database or configured file system of the Bitcoin client. The advantage of this key management is the quick and easy access of the keys for any Bitcoin transaction but this kind of systems is not safe from the online hackers, malicious software stored on the device, physical access and physical damage of the device.

Password Protected Wallet In this kind of system, keys are protected by the user created password. Stored keys are usable by the Bitcoin software only if correct password is supplied to access the keys. In case of un-authorized physical access of the device, password resists to illegitimate access of the stored keys. However, this kind of solution is breakable by stealing the keys through key stroke software and bruit force attack. The major drawback of this kind of key management system is that if owner of the wallet forgets the password then he/she losses the Bitcoin balance of his/her Bitcoin wallet.

Offline Key Storage To avoid the possibility of online hacking of keys, stealing of keys through malicious software and physical access of the device in local key storage mechanism, private keys are stored in the offline portable media like USB or in form of paper wallet. In paper wallet, keys are stored on paper in form of bar codes. However, drawback of this kind of storage is that wallet is not immediate accessible.

Password Driven Keys In this Key Management approach, user provided password is used to drive the public–private key pair to operate the Bitcoin wallet. The major drawback of this key management approach is the exhaustive search on public–private key pair through Rainbow table attack. In rainbow table attack, table of public–private key pair is generated for all possible passwords for a specified length. If password is weak then private key can be easily found using the Rainbow table attack.

Hosted Wallet In this approach, account detail of the user is hosted on the web server hosted by the third party. Using web authentication mechanism, user accesses the Bitcoin Wallet services. In this approach the security of the Wallet is in hand of third party so it is advisable to keep small amount in such Wallets.

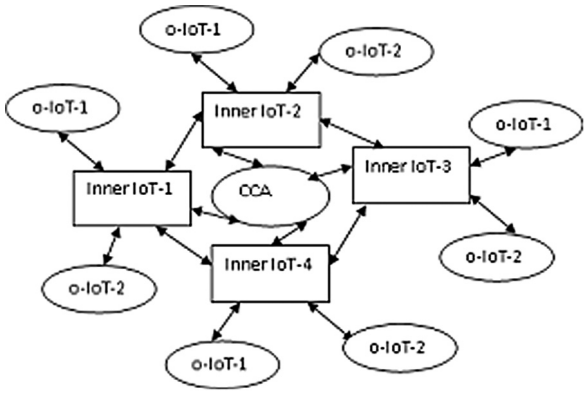

Fig. 3. Two layered blockchain architecture.

2.2. PKI for blockchain

Public Key Infrastructure (PKI) is one of the mechanism to manage the keys in the public key cryptographic systems. Blockchain also utilizes the services of third party through PKI to authenticate the nodes of the Blockchain network. There are many Blockchain based PKI approaches in the field of Blockchain Technology which reduce the dependency on third party for authenticating the nodes. However, minimizing the dependency on third party by using the efficient key management is still a big challenge in the field of Blockchain Technology. Following are some major Blockchain based PKI approaches-

Multi-Layered Approach Gan [12] proposed a two layered Blockchain architecture in which inner layer IoT nodes have higher privileges than outer layer IoT nodes. For adding any IoT node in inner layer, Centralized CA (CCA) is responsible. Inner layer IoT nodes are responsible for adding the IoT nodes in the outer layer using the PKI. CCA stores the public keys of inner layer IoT nodes and inner layer IoT nodes store the public keys of the outer layer IoT nodes. (See Fig. 3.)

Instant Karma PKI In this approach, CA is responsible to authenticate the Blockchain IoT nodes [13]. However, in this approach behavior of the CA is recorded in the form of Blockchain record with the consensus of the existing nodes. Misbehave activity of the CA is determined by the majority consensus of the existing nodes.

Guardtime Approach In this approach [17] a Physical Unclonable Function (PUF) is used to identify the IoT device. PUF is a function which uses the physical property of the device for generating the desired output. Using generated desired output from the physical property of IoT device, a unique private/public key pair is generated and this generated pair is used in Blockchain infrastructure. Therefore, IoT nodes are not fully dependent on the CA.

3. Proposed group key management for blockchain network

Preservation of the confidentiality of sensitive transactions and efficient encryption of payload are also major challenges

Please cite this article as: O. Pal, B. Alam, V. Thakur et al., Key management for blockchain technology, ICT Express (2019), https://doi.org/10.1016/j.icte.2019.08.002.

Table 1
Notations.

Notation	Description
GK	Group key
Code (i, j, k)	Group identification code
$GK_{i,j,k}$	Group Key of the group which have code (i, j, k)
c_l	lth children
f (.)	One-way cryptographic function which generates the output of length d

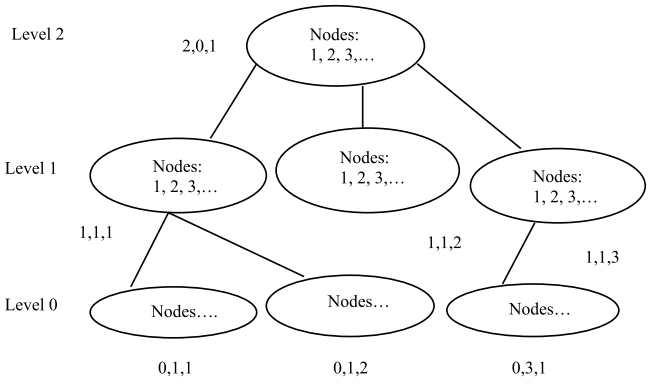

Fig. 4. GKM framework.

of the consensus phase of the Blockchain Technology. To ensure the confidentiality and efficient encryption of payload during consensus phase, we propose a secure and efficient Group Key Management (GKM) framework for Blockchain Technology. Notations used are given in Table 1. When multiple domains are connected through single layered architecture then some of the transactions of one domain may not contribute any value to other domains. In such scenario, multi-layered architecture is a preferable approach. In our proposed GKM framework, we assumed the multi-layered architecture in which nodes of upper layer have more privileges and rights than the nodes of the lower level.

At each level, there are multiple groups and each group contains the multiple nodes. Nodes belong to the same group have the same privileges. At lower level, nodes join the group with the consensus of nodes of parent group. Proposed framework is given below-

Each group of GKM framework is represented by a code (i, j, k) where i denotes the level, j denotes the position of parent group in upper layer and k denotes the position of the group in current layer under the parent group. Let $GK_{i,j,k}$ represent the Group Key (GK) of the group having the code (i, j, k) and this GK is used to encrypt or decrypt the common messages for the group members who belong to the group having code (i, j, k).

At level 0, Group Keys are assigned to each group. In Fig. 4 Group Keys $GK_{0,1,1}$, $GK_{0,1,2}$ and $GK_{0,3,1}$ are assigned to groups who have codes (0, 1, 1), (0, 1, 2) and (0, 3, 1) respectively. Group Keys of groups of higher layers (other than level 0) are computed using the group keys of child groups using the one-way function. One-way function f(.) generates the output of length d therefore, length of $GK_{i,j,k}$ is also d.

Let $c_1, c_2, \ldots, c_l$ be the children of the group having the code (i, j, k) then $GK_{i,j,k}$ is computed in the following way-

$$GK_{i,j,k} = f\left(GK_{i-1,k,c_1}, GK_{i-1,k,c_2}, \ldots\ldots GK_{i-1,k,c_l}\right)$$

Parent groups have higher privileges and they can view the confidential data of the children groups. No group can access confidential data of parent groups and groups which are at same layer. To manage the GKM network, root group assigns the GKs to the groups which are at level 0 with the consensus of members of the root group. In case of any membership change for any group, root group updates the concerned group keys with consensus of members of root group.

In proposed framework transactions are open to all members of the concerned group as well as for members of the parent group but for non-members, transactions are confidential. Proposed framework contains all benefits of Blockchain Technology with restriction on openness for non-members.

3.1. Security analysis

Function f(·) is a one directional function which takes the input of two or more values. Length of each input value is d. f(·) produces the output of fixed length bit string of length d. Let intruder may try to revert the function z = f(w) to obtain the value w if intruder has value of z but it is not possible because z is confidential for non-members and length d is sufficiently large. It is also not possible to obtain the input w if z and f(·) are available i.e. one-way function is irreversible. It is not possible to have input w′ in such a way that z = f(w) = f(w′). It is impossible to get output z = f(w′) when w′≠ w. Therefore, it is concluded that proposed mechanism is secure.

4. Conclusion

Blockchain Technology has the tremendous potential to transform the existing business process, e-Governance services, financial services, health care services, agriculture services etc. into new dimensions where additional advantages in terms of efficiency, cost, trust, security, integrity of data etc. are guaranteed. Blockchain technology eliminates the need of third party to validate the transactions over the network.

In this paper we discussed the Blockchain Technology and its uses for IoT systems. We also discussed the need of Key Management for Blockchain which includes the key management for Bitcoin currency wallet and Blockchain Public Key Infrastructure.

Please cite this article as: O. Pal, B. Alam, V. Thakur et al., Key management for blockchain technology, ICT Express (2019), https://doi.org/10.1016/j.icte.2019.08.002.

In addition to authentication of Blockchain nodes, it is also necessary to ensure the confidentiality of the sensitive transactions over the Blockchain network. To address the issue of confidentiality of sensitive records, we proposed a Group Key Management (GKM) scheme for secure group communication.

Declaration of competing interest

The authors declare that there is no conflict of interest in this paper.

References

[1] S.T. Aras, V. Kulkarni, Blockchain and its applications — A detailed survey, Int. J. Compt. Appl. 180 (3) (2017) 0975–8887.
[2] S. Huckle, R. Bhattacharya, M. White, N. Beloff, Internet of Things, blockchain and shared economy applications, Presented in Proceedings of International Workshop on Data Mining in IoT Systems, ScienceDirect, Procedia Comput. Sci. 98 (2016).
[3] J.H. Park, J.H. Park, Blockchain Security in Cloud Computing: Use Cases, Challenges, and Solutions, Symmetry, 2017.
[4] A. Azaria, A. Ekblaw, T. Vieira, A. Lippman, MedRec: Using blockchain for medical data access and permission management, in: Proceedings of 2nd International Conference on Open and Big Data, 2016.
[5] R.-H. Hsu, J. Lee, T.Q.S. Quek, J.-C. Chen, Reconfigurable Security: Edge Computing-Based Framework for IoT, [cs.CR], 2017.
[6] The Future of Public Service Identity: Blockchain, report of M/s Accenture, 2017.
[7] I.-C. Lin, T.-C. Liao, A survey of blockchain security issues and challenges, Int. J. Netw. Secur. 19 (5) (2017) 653–659.
[8] S. Huh, S. Cho, S. Kim, Managing IoT devices using blockchain platform, in: ICACT2017 February 19–22, 2017.
[9] Survey on Blockchain Technologies and Related Services, Nomura Research Institute, Japan's Ministry of Economy, Trade and Industry (METI), 2016.
[10] Z. Zheng, H.-N. Dai, S. Xie, Blockchain challenges and opportunities: A survey, Int. J. Web Grid Serv. (2017).
[11] T. Salman, M. Zolanvari, A. Erbad, R. Jain, M. Samaka, Security services using blockchain: A state of the art survey, IEEE Commun. Surv. Tutor. (2018).
[12] S. Gan, An IoT Simulator in NS3 and a Key Based Authentication Architecture for IoT Devices using Blockchain, Indian Institute of Technology, Kanpur, 2017, [online]. https://security.cse.iitk.ac.in/node/240. (Accessed February 28, 2019).
[13] S. Matsumoto, R.M. Reischuk, IKP: turning a PKI around with decentralized automated incentives, in: 2017 IEEE Symposium on Security and Privacy, SP, San Jose, CA, 2017, pp. 410–426.
[14] G. Zyskind, O. Nathan, Alex 'Sandy' Pentland: Decentralizing privacy: Using blockchain to protect personal data, in: Proceedings of IEEE CS Security and Privacy Workshops, 2015.
[15] C. Fischione, Lecture Note on Consensus Algorithms, Royal Institute of Technology –KTH Stockholm, Swedene.
[16] S. Eskandari, D. Barreray, E. Stobertz, J. Clark, First look at the usability of Bitcoin key management, arXiv:180204351 [cs.CR], http://dx.doi.org/10.14722/usec.201523015.
[17] Guardtime, Internet of Things Authentication: A Blockchain Solution using SRAM Physical Unclonable Functions, 2017, [online]. https://www.intrinsic-id.com/wpcontent/uploads/2017/05/gt_KSI-PUF-web-1611pdf. (Accessed February 28, 2019).
[18] A. Lewko, B. Waters, Unbounded HIBE and attribute-based encryption, in: Advances in Cryptology - EUROCRYPT, vol. 6632, Springer Berlin Heidelberg, 2011, pp. 547–567.
[19] N. Fotiou, G.C. Polyzos, Decentralized name-based security for content distribution using blockchains, in: 2016 IEEE Conference on Computer Communications Workshops, INFOCOM WKSHPS, San Francisco, CA, 2016, pp. 415–420.
[20] A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, P. Chibueze, A, Ogah, Z. Sun, Blockchain-based dynamic key management for heterogeous intelligent transportation systems, IEEE Internet Things J. 4 (6) (2017).
[21] J. Brito, Bitcoin APrimer for Policymakers, 2013.
[22] Blockchain Tech Beyond Bitcoin, Sutardja Center for Entrepreneurship & Technology Technical Report, 2015.
[23] J. Billings, Image-Based Proof of Work Algorithm for the Incentivization of Blockchain Archival of Interesting Images, University of Colorado Denver.

Please cite this article as: O. Pal, B. Alam, V. Thakur et al., Key management for blockchain technology, ICT Express (2019), https://doi.org/10.1016/j.icte.2019.08.002.