International Journal of Engineering Science Invention (IJESI)
ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726
www.ijesi.org ||Volume 7 Issue 1|| January 2018 || PP. 50-52

Confidentiality in Blockchain

Ayyub Ali[1], Dr.Mohammad Mazhar Afzal[2]
Department of Computer Science and Engineering, Glocal University, Saharanpur
Corresponding Author: Ayyub Ali[1]

Abstract: *Blockchain technology is one of the frequently discussed technologies in the recent years. It is changing the life style and way of thinking of the people. Due to its nature of free from control of central unit it has impacted in many fields from business to education and financial organizations. It's a bunch of features that makes it like a rising star in the field of technology. But then also we have to concern about the privacy and confidentiality challenges in this technology.*

Keywords: *Blockchain, Privacy, Security, Confidentiality*

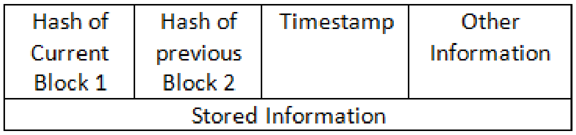
Date of Submission: 29-12-2017 Date of acceptance: 11-01-2018

I. Introduction

Started from the digital currency blockchain has been applied to many fields. So it's very important to think about the privacy rules and security when planning to accept a blockchain system. Privacy and security is the matter of great concern in the design of a blockchain. As blockchain deals with storage and exchange of information, which may be personal information. The privacy and security rules must be applied to the processing of information via blockchain. In blockchain, privacy and confidentiality refers that transaction and details of the nodes are safe.

1. Blockchain

Blockchain is the latest way of sharing and storing information. This technology uses different way of storing the data that is different from other traditional methods. The blockchain technology is a good example of security (in terms of immutability) and privacy. The information is stored in the form of blocks and these blocks are connected with each other. Newly generated block is to be connected to its previous block, in this way it makes a chain of blocks. The information stored in the block is permanent i.e. it can't be alter or modify. To make any change in the stored information is a very typical task. Because all participating nodes must be agree for update.



Hash of Current Block 1	Hash of previous Block 2	Timestamp	Other Information
Stored Information			

Fig 1: A block structure

Every block contains a hash of the previous block. A hash is sequence of numbers and characters. T*ransparency and verifiability* help to prevent unauthorized changes.

There are many features that make the blockchain technology more attractive for financial use cases in terms of confidentiality and privacy:

- Avoids the need of a middle-man which can reduce transfer cost.
- Supports for digital transactions.
- Creates an open ledger, which makes it easier to share information with in the network.

2. Confidentiality and Privacy versus Security

CIA tried model is followed in an organization to achieve the data security. CIA stands for Confidentiality, integrity and availability. Confidentiality means limiting the access to information. That is only authorized person can access the information. The means of integrity is that the information is trustworthy and accurate. The information is not modified by any bad actor. The integrity is the way of maintaining the consistency, accuracy, and trustworthiness of information over its entire life cycle. The availability means that the information will be available when required. Blockchain technology fulfills the requirement of both integrity and availability, but achieving confidentiality has proven to be more challenging.

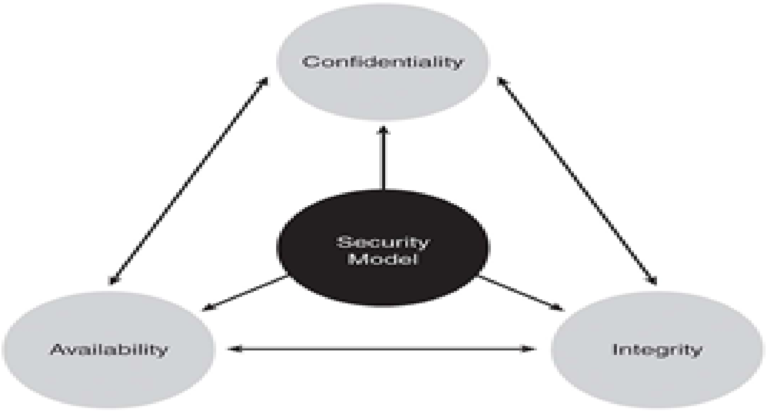


Fig 2: CIA triad

The **confidentiality and privacy** means the data is protected. In terms of blockchain technology, confidentiality and privacy means that both the transaction and the identities of participating nodes are protected. To achieve the requirements of any system it must satisfy the following:

- An unauthorized third party should be able to identify the counterparties to a transaction in a blockchain until unless the counterparties reveal that information.
- Transaction details must be invisible to the person who is not involved in that particular transaction until the participating parties not disclose their information.

Integrity means the data that is written to the blockchain is correct and cannot be subsequently altered:

- Only authorized parties can add the transactions in a blockchain.
- Once a transaction is committed it can’t be denied later.
- Every transaction is immutable i.e. it’s not easy to edit a transaction after completion the transaction
- Any transaction cannot be cancelled or reversed.

Availability of blockchain systems refers to their ability to withstand outages and attacks:

- In a blockchain the information should be available at all participating nodes without any failure. This is inherent in blockchain technologies’ distributed nature.
- The system must have the capacity of handling high loads in its working condition.

3. Privacy

In a blockchain all transactions are published publically and they are available for all participating nodes in the system. In most applications the published transactions are not encrypted. If this information is important related to someone or its personal data, this creates the regulatory and legal problems. We can store data in encrypted form for its security. But it’s not the right solution of the problem. Because we are human, we can lose the decryption key or can forget. In these cases the data may not be recovered in its original form. All decrypted data will be decrypted forever since the data cannot be altered. In case of a public blockchain ledger is publically available. *Anyone* can look at this ledger and see what the balance of a specific address is.

Here fig 3. shows the example of transaction of Bitcoin from a sender A to a receiver B. Here A sends details of the transaction publically and every node is able to see the details of this transaction along with the receiver B. In his way every node is able to guess how much money A and B have. And this is not good.

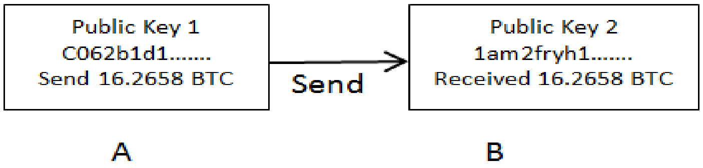


Fig 3: Transaction of Bitcoin

We need to encrypt the information in a transaction to make information *much* more private. To add this encrypted information, we need to add more data to each individual transaction on the network. But it's not so easy because it will increase the size of a current transaction. Also if we send the encrypted form of transaction this is not good practice of blockchain. Because in a blockchain ledger must be opened. The fig 3 shows detail of a transaction in a Bitcoin blockchain. From this transaction we can see how the information in a blockchain is published publically and the addresses of communicating parties are linked across multiple transactions. The transactions are publically published, open and transparent. So with the help of this public key any how someone can get the details of the transaction of a particular body and his account. In a public blockchain transaction details are not confidential.

II. Conclusion

Blockchain technology has had proven success with providing integrity and trust, while other properties like scalability, confidentiality and privacy are less mature and active areas of research and development. This survey focused on confidentiality and privacy, covering the different technologies that are being used and developed today to make blockchains more private and confidential.

References

[1]. Shrier, D., Wu, W. & Pentland, A. Blockchain & Infrastructure (Identity , Data Security). 1–19 (2016).
[2]. EU. (2016). Blockchain applications & services. Case study.
[3]. B. Schoenmakers, Security aspects of the ecash payment system, Lecture Notes
[4]. in Comput. Sci. (1998) 338–352. http://dx.doi.org/10.1007/3-540-49248-8_16
[5]. Iqra Basharat, Farooque Azam, Abdul Wahab Muzaffar,"Database Security and Encryption: A Survey Study", International Journal of Computer Applications (0975 – 888) Volume 47– No.12, June 2012.
[6]. G. Maxwell, Coinjoin: Bitcoin privacy for the real world, 2013. https://bitcointalk.org/index.php?topic=279249.0.2013.

International Journal of Engineering Science Invention (IJESI) is UGC approved Journal with Sl. No. 3822, Journal no. 43302.

Ayyub Ali. " Confidentiality in Blockchain." International Journal of Engineering Science Invention (IJESI), vol. 07, no. 01, 2018, pp. 50–52.