Necessary requirements for Blockchain Technology and its Applications

Article · April 2018

CITATIONS
4

READS
542

2 authors, including:

Venkatesh Kanyakumari
Myanmar Institute of Information Technology Myanmar
69 PUBLICATIONS **55** CITATIONS

SEE PROFILE

International Journal of Computing Science and Information Technology, 2018
ISSN: 2278-9669, April 2018 (http://ijcsit.org)

Necessary requirements for Blockchain Technology and its Applications

Ms. Sheetal[1], Dr. K. A. Venkatesh[2]
Research Scholar, Presidency University, Bengaluru, India
Sheetal.sunil@gmail.com

Abstract

Blockchain technology is a innovative and secured by cryptographic algorithms, distributed database and digital ledger. Blockchain technology is replacing the traditional/Centralised database which is being used. This paper just focuses on prerequisite for blockchain technology, Awareness of the technology and also gives an idea whether to choose blockchain technology as right solution for an application with necessary requirements for its implementation (Set Up). We have also proposed an application implemented by Blockchain Technology. Discussed different cases yet to implement by blockcahin and already implemented in action.

Keywords: Blockchain, Hashing, Digital Ledger, Proof of work and proof of stake and criminal records.

1. INTRODUCTION

Due to lack of trust in third party or just to remove trust on a third party which is involved in maintaining our data or transactions a new innovative method provides a solution by replacing a traditional centralised database into distributed database without third party involved which is capable of maintaining record or transaction and for blocks which are verified and added to a chain of network. Each block is then linked to the next block, using cryptographic algorithms and hashing techniques. The initial block is referred as genesis block. These blocks are accessible to all the nodes present in the network which is distributed in nature. The data blocks are irreversible and the consensus mechanism makes it fraud free and trust worthy without third party. In this paper, we analyse the properties such as transaction speed, control over

Blockchain network of different blockchain types (i.e. permissioned and permissionless) and comparative study properties to those of a centrally managed database. We provide a decision tree to identify whether a blockchain is useful depending on the problem requirements, and if so, what type of blockchain might be appropriate and also step by step procedure requirements of blockchain technology.

2. BACKGROUND ON BLOCKCHAIN

In the following section, we detail the required blockchain background.

In 2008 Satoshi Nakamoto figured out how to implement a digital, distributed, with the ideals of cryptographic algorithms, hashing techniques and released software called blockchain technology. Bit coin is the earliest application of Block Chain Technology. It serves as protocol for exchanging crypto currencies such as Bitcoins. It solves very well-known computer science problem "Byzantine Generals Problem" which questioned the consensus of distributed system by providing a solution.

2.1 Centralized database: A third party organization will be involved to maintain the database

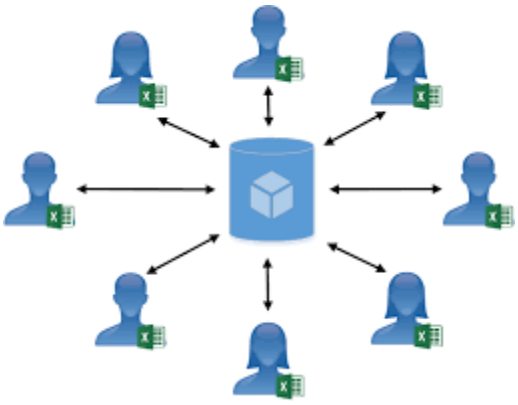

Fig. 1: Centralised database

2.2 Blockchain Ledgers

2.2.1 [2] Permissioned blockchain Mining makes the blockchain to be Permissioned and permissionless. The permissioned block is mined by the known miners who have authority. The authority of a miner can be controlled in permissioned block. Every component

permissioned block can be customised for a permissioned platform. Verification of transcation is done by authorized members. So, practically the ledger does not require a consensus scheme to ensure tamper resilience. To only authorized and limited set of members in the network are given rights to view content of the block so called readers and authorized writers to update the transaction, this concept in blockchain can be referred as permissioned blockchains. To implement a permissioned ledger designs to be considered as follows:

a) Identifying the participants in the Network and their role
b) The structure of every type of transaction to be used in the network, and the appropriate algorithms to verify each transaction in the network.
c) Designing the structure to control the network with certain rules for deciding who is authorized user to access control and the actions in the network to be performed by their members for each type of transaction.
d) Designing the control structure for authorized miner so as to control who can mine a block and which transactions can be included in the network
e) Designing the structure for each member in the network that defines rights of viewing the content of the blocks, and to verify block.
f) Designing an appropriate consensus algorithm and an incentive scheme or reward to ensure the honesty of the members in the network, if required to make it fraud free. The design choices can be made based on the type of applications. Example of permissioned blockchain are Hyperledger Fabric and R3 Corda [4].

2.2.2 Permission less blockchain:

They are decentralized Network and open to all members in the network. Any node can join and leave the network. There is no control for accessing the block to view the transactions anyone in the network has right to read. The right to update the transaction is given to all in the network ie. anyone can be writer at any time. There is no central entity which manages the membership, or which could decide the readers or writers. The use of cryptographic algorithms will help to design the structure of such a permissionless blockchain that makes sure of network to be secure

Example of permissionless blockchains such as Bitcoin [2] and Ethereum [2].

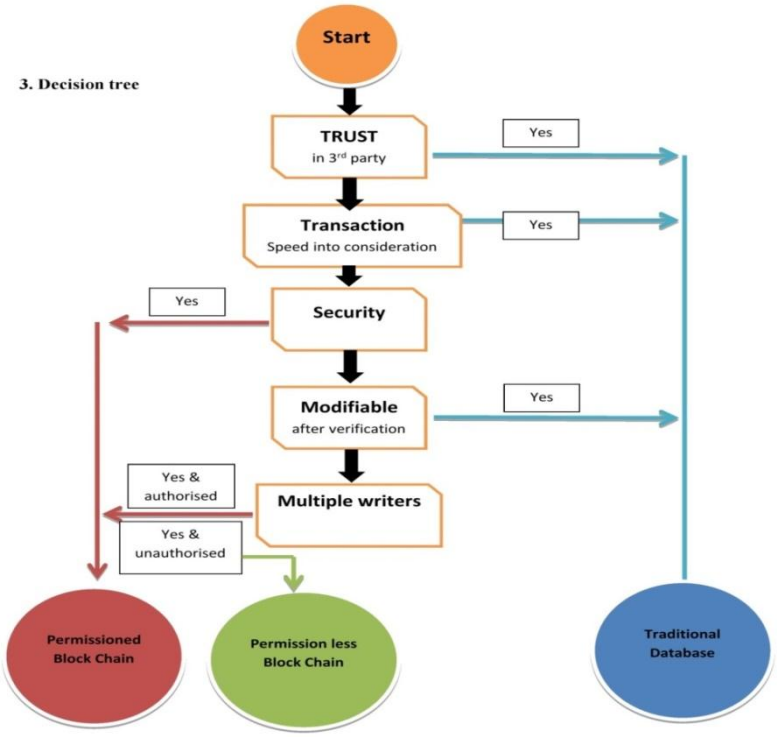

Fig. 2: A flow chart to determine whether a blockchain is the appropriate technical solution to solve a problem. A Consensus is the algorithm is provided and verified by honest participant and is referred as writers who can add blocks by mining. The members who can view the transactions in the network are referred as reader.

4. Requirements for implementation of Blockchain technology

4.1 Software

A Software program which consists of following functions

a) Create own Hash function
b) A function that generates public key and private key.

4.2 Transaction ledger

Each block should consist of Block Number and every block should contain of number of transactions. Each transaction should contain unique transaction ID. Transaction details containing Public key of the sender, public key of the receiver referred as message. Input the amount and the fees for the transaction. Output the total balance available.

Example: Sender wants to send 10 btc to receiver

Input = 10 btc to receiver

Miner/ transaction fee = 1 btc (10btc-1btc)

Output is 9btc which receiver can have in his bitcoin wallet.

4.3 Cryptographic algorithms for Hashing

Method or technique used for Hashing. SHA 256 is used. The hash begins with number of zero bits. The **SHA** (Secure Hash Algorithm) is one of a number of cryptographic hash functions. A cryptographic hash is like a signature for a text or a data file. **SHA-256** algorithm generates an almost-unique, fixed size **256**-bit (32-byte) hash. Hash is a one way function – it cannot be decrypted back.

4.4 Verifying the transaction

Proof of work: (One CPU is one vote) PoW is the consensus algorithm used in bitcoin. Its core idea is to allocate the accounting rights and rewards through the hashing power competition among the nodes. This depends on the amount of processing power donated to the network

Proof of stake: In PoS the digital currency has the concept of coin age. Coin age of a coin is its value multiplied by the time period after it is created. The longer one node holds the coins, the more rights it can get in the network.

4.5 Network

Decentralized Network: Steps to run the Network are as follows:

a) New transaction are broadcast to all nodes

b) Each node collects new transaction into a new block.

c) Each node works on finding a difficult proof-of-work for its block.

d) When a node finds a proof-of-work, it broadcasts the block to all nodes.

e) Nodes accept the block only if all transactions in it are valid and not already spent.

f) Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.[1]

5. Blockchain in action: Use cases

Case 1: Indian companies using blockchain technology to better services : Several Financial services in India has started using Blockchain Technology. One among that is Bajaj Finserv, the holding company of Bajaj Group's and insurance firms, is using blockchain technology for several services like travel insurance and for settling claims.[9]

Case 2: ICICI Bank executes India's first banking transactions on blockchain in partnership with Emirates NBD

Mumbai: ICICI Bank in India recognised as largest private sector bank by consolidated assets, has already implemented and announced that it has successfully executed transactions in international trade finance and remittance using blockchain technology in partnership with Emirates NBD, a leading banking group in the Middle East.

ICICI Bank is the first bank in the country to implement using blockchain technology. Documents related to purchase order, invoice, shipping & insurance, among others, electronically on blockchain in real time. The usage of blockchain technology simplifies the process and makes it almost easy—to only a few minutes. [10]

Case 3: A leading consumer equipment manufacturing company in India has started using Blockchain to make payments to their suppliers.. The process for bill discounting has reduced and transactions have become completely digital and paperless.

6.Proposed Applications using Blockchain

[11]Case 1: Several tech experts have suggested using emerging and contemporary technologies in EVMs rather than the one that are being using currently. One of the most commonly suggested technology by tech experts in India that can solve the EVM tampering debates all at once is blockchain..

[12] Case 2: Blockchain is used for land dealings t into the larger mandate of e-governance in India. Many other state governments are exploring the usage of the technology, Andhra Pradesh is leading the state to use blockchain by conducting trials within its departments. The state is working with startups such as Snapper Technologies and SimplyFy to implement blockchain across administrative processes.

7. Our Proposal: Storing criminal records using Blockchain technology:

Police stations and investigating bureau can use blockchain technology to maintain criminal records. Once the record is stored cannot be manipulated. Store once and can be accessed by anyone in the network. It is open, transparent easy to track the record of the criminal by the investigating officer. It provides users the ability to manipulate the ledger in a safe way without seeking the support of a third party.. Blockchain's algorithm reduces the dependence on people to verify the transactions. Due to open network any police station across the network can access the crime details easily. The node that is honest in storing and verifying the record should be rewarded by score. Score sheets can be considered for promotions and so on. Common man also should be given opportunity to access the network in case if any he/she knowing some valid information about the criminal which has to be verified and can be considered as evidence.

8. CONCLUSION

In this paper we provide the structured methodology to decide which technological solution to be adopted depending on the type of solution we are trying to solve in our problem. The choice of type of database to be used is discussed before as due to hype created for blockchain[7]. Few properties are considered to design the decision tree such as the required trust assumptions, Transaction speed, security, modifiable mode after adding the block to the chain and control access over the transactions in the network. We conclude this with basic requirements to be used to set up a block chain depending on the type of application. We have also proposed an application that can be implemented using Blockchain technology.

REFERENCES

[1] S. Nakamoto, "Bitcoin: A peer-to-peer Electronic cash system," *Article*, 2008.

[2] IDRBT by RBI, " White paper: Applications of Blockchain technology to banking and financial sector in India.," 2017.

[3] https://en.wikipedia.org/wiki/SHA-2

[4] Richard Gendal Brown, James Carlyle, Ian Grigg, and Mike Hearn. Corda: An introduction. R3 CEV, August, 2016.

[5] A. G. Karl Wüst, "Do you need a Blockchain?," 2016.

[6] M. E. Peck, "Do you really need a blockchain?," https://spectrum.ieee.org/computing/networks/do-you-need-a-blockchain, 2017.

[7] Gideon Greenspan. "Avoiding the pointless blockchain project", 2015.http://www.multichain.com/blog/2015/11/avoiding-pointlessblockchain-project/.

[8] Reuben Grinberg , 2011. Bitcoin: "An innovative Alternative digital currency" (Hastings science & technology law of Journal, Volume: 4:1)

[9]https://economictimes.indiatimes.com/news/company/corporate-trends/indian-companies-using-blockchain-technology-to-better-services/articleshow/61509547.cms

[10]https://www.icicibank.com/aboutus/article.page?identifier=news-icici-bank-executes-indias-first-banking-transactions-on-blockchain-in-partnership-with-emirates-nbd-20161210162515562

[11]https://www.indianweb2.com/2017/06/27/election-commission-use-blockchain-technology-voting-machines/

[12]https://www.forbes.com/sites/sindhujabalaji/2017/12/28/indias-blockchain-revolution-goes-beyond-banks/#6525ca074123.