International Journal of Engineering Research and Management (IJERM) – Volume-4, Issue-1, March 2018

Decentralized Security Framework Using Blockchain Mechanism

Sneha S. Mande[#1]

[1]M.E.Student, Computer Department, S.V.I.T, Nashik, Maharashtra, India

[1]mandesneha009@gmail.com

Abstract - *A Blockchain is basically a centralized, distributed ledger of all the transactions or events which takes place only after involving multiple parties. It ensures high level of security as the transactions which take place are entirely anonymous. Blockchain service holds a great promise to improve many different industries, yet there are significant cyber security concerns which must be addressed. It enables new forms of distributed software architectures, where agreement on shared states can be established without trusting a central integration point. As a database and computational platform, blockchain has both advantages and disadvantages compared with conventional techniques. Blockchain may be an appropriate choice for some use cases while conventional technologies will be more appropriate for other use cases. This paper proposes a new reputation system for data credibility assessment based on the blockchain techniques. In this system, vehicles rate the received messages based on observations of traffic environments and pack these ratings into a "block". Each block is "chained" to the previous one by storing the hash value of the previous block. Then, a temporary center node is elected from vehicles and it is responsible for broadcasting its rating block to others. Based on ratings stored in the blockchain, vehicles are able to calculate the reputation value of the message sender and then evaluate the credibility of the message.*

Keywords — *decentralized, distributed, ledger, Blockchain, cyber security, data credibility.y*

I. INTRODUCTION

The blockchain is one of the most emerging technologies of cyber security. This technology has successfully replaced economic transaction systems in various organizations and has the potential to revamp heterogeneous business models in different industries. It promises a secure distributed framework to facilitate sharing, exchanging, and the integration of information across all users and third parties, it is important for the planners and decision maker to analyse it in depth for its suitability in their industry and business applications. Blockchain is a decentralized ledger or data structure. It can be referred as blocks in a chain where the corresponding blocks refer to the blocks, prior to them. Once the details of the transactions or events are fed into the Blockchain, it is impossible to tamper the details are shared with the members of the network. Users of the Blockchain network should be completely aware of the transactions taking place. We will draw an analogy to justify the concept. We consider it to be a book based data structure where each page of the book refers to its previous page by a page. Here, book refers to the Blockchain, page refers to the book and an entry in any page refers to the blockchain transaction. It is easy to detect whether a page or a block has been tampered or not. Pages can be arranged in any manner so pages aren't important in a distributed ledger. In blockchain, each block is built on top of the previous block and it uses the latter's nonce and signature as a key for going into the next block.

A. Advantages of Blockchain

The Blockchain protocols featured are listed below:

1) Immutable: It means that it is really difficult to tamper or alter a block.
2) Irreversible: It prevents double spending.
3) Distributed system: It means that a copy of the ledger is present with all its members.
4) No Centralized Authority: It is a peer to peer system.
5) Resilient: It is not prone to any sort of major attacks.

II. BLOCKCHAIN TECHNOLOGIES

Blockchain are working on different kind of technologies. Few of them are listed below:

A. Colored Coins

Protocols allow the digital assets other than Bitcoin to be transferred in the Bitcoin blockchain using the Bitcoins as "tokens". Bitcoins can be used as a transfer the element for the Bitcoin transaction where it can be regarded as a meta data for representation of shares, property and other instances.

B. Ethereum Blockchain

It is a new developed Blockchain and it operates using digital contracts known as "Smart Contracts". The protocol for Ethereum is different from Bitcoin Blockchain. Smart Contracts are basically small computer programs that accounts for a deal between a client and an end user. Blockchain has a wide range of financial and non financial applications.

It has been used largely by Multinational companies like IBM, Amazon etc. and will be used further in the coming years. Many banks have collaborated in order to implement Blockchain technologies in their system.

C. Alternative Blokchains

This is also termed as "Sidechains". In the Alternative Blockchain feature, we can shift the bitcoins of the Bitcoin Blockchain to a new Blockchain. We can transfer using Bitcoins having said that, we have to adapt to the new rulesmas well. We might have lesser time for Validation, more easily programmable and most importantly, a separate consensus mechanism. It ensures user scalability.

D. Hyperledger Blockchain

It is an umbrella project of Open Source Blockchain and related tools , started in 2015 by Linux Foundation to support the collaborative development of Blockchain based Distributed ledgers. It has four platforms like Iroha, Fabric, Sawtooth and Burrow. IBM owns the Hyperledger Fabric and Intel owns the sawtooth project of Hyperledger.

III. WORKING OF BLOCKCHAIN

Blockchain is considered to be the next big revolutionizing technology, as it is reinventing the way we work and live. The idea of the blockchain was first introduced by a researcher who implemented the digital crypto currency known as bitcoin. Blockchain has become an integral part of bitcoin's operation. For several decades, we have been dealing with information exchange and the transfer of money and other assets through online transactions via the Internet, where each of these transactions involved a trusted intermediary. It is responsible for guaranteeing a secure exchange and are accountable in the event of any failures or security breaches. In a paradigm shift, the blockchain eliminates the need for any central authority between multiple parties executing financial and data transactions by using an incorruptible, immutable, and decentralized public ledger.

Bitcoin uses proof under Cryptographic primitives rather than entirely trusting on the third party. Hence, "digital signature is introduced". The sender sends using his private key and the receiver receives it using his public key and the person needs to know the private key and the digital signature. The peer nodes present in the Bitcoin network is completely aware of the transactions which take place. The transactions must be "endorsed" and "validated" in order to be reflected in a public ledger. The admin must know that the sender has the right to spend it. Also, the admin must be aware that the sender has enough money in his account to make a "legit" transaction. The transactions in a Bitcoin network are not ordered. Thus, there is a chance of double spending and it can be removed by the introduction of Blockchain Technology. In Blockchain, the transactions are ordered in form of blocks in a linear chain, which are linked to each other. Every block contains the hash of the block prior to it. We have introduced a concept called "Proof of Work". The task of the node is to find the random string or nonce. This random string has to be hashed with the transactions and the hashes of the previous blocks and then, it produces a hash with certain number of leading zeroes.

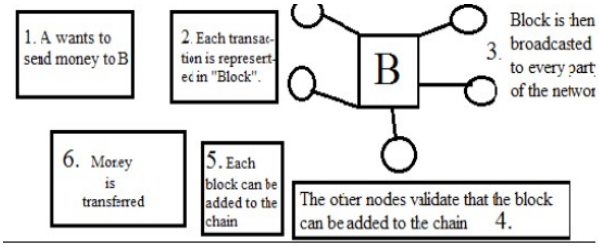

Fig.1. Workflow of the Blockchain Mechanism

IV. EVALUATION FRAMEWORK

The process to evaluate the suitability of blockchain mainly consists seven questions which need to be answered, which are denoted as white decision nodes. The sub questions derived from the main questions are denoted as grey decision nodes.

A. Multi-party

The question is whether multiple parties are involved in the scenario. Operations or transactions between parties are normally governed by intermediaries. Supply chain is the examples as it consists of complex, dynamic, multi-party arrangements with regulatory and logistical constraints spanning across different jurisdictional boundaries. Blockchain provides a shared infrastructure with a neutral stand where none of the participated organization dictates it. Blockchain is suitable for scenarios which involves multiple parties, potentially where there are intermediaries acting within the current systems. It can break down the silos of information controlled by individual parties while at the same time we can make the process faster and cheaper. A system within a single entity can use other relatively cheaper mechanisms to achieve the same properties provided by blockchains.

B. Trusted authority

The next question is whether a trusted authority is needed in the scenario. Trusted authority is an entity that is authorized to execute a certain operation or alter a policy or configuration of an operation. The trusted authorities would be the bank and government. The issue arises from having a

trusted authority is that it may become a single point of failure. If the trusted authority experiences problems, all the users accessing the services from it would be affected. Blockchain is suitable for scenarios without any trusted authority or the current trusted authority has potential to be decentralized. Blockchain does not remove trust because users are still exposed to risk in their use of blockchain technology. Users are moving their trust from the third-party or central governing organization to the blockchain software, the incentive that motivates "good behaviour" of the processing nodes, and the trusted third parties that act as "oracles" which record information about the external world on the blockchain. Blockchain removes the need to trust a single specific third party to maintain the ledger of a transaction, and so is sometimes called a "distributed trust".

C. Centralized operation

In blockchain-based systems uses smart contracts, system operation is harder to implement for the smart contracts than regular distributed systems. Since smart contracts comprise code that regulates the interactions between mutually untrusting parties.

Using blockchain-based system, no single party controls the system but every single user is in control of their own data and assets, which creates challenges for governance. The management of the evolution of blockchain based systems is more like diplomacy than traditional risk management or conventional product management. Hence, the current configuration of blockchain is not suitable for a system that requires centralized operation.

D. Confidentiality vs Data

The important question is whether data transparency or confidentiality is required. Blockchain provides a neutral platform where all participants can see the published data. With all the published information, transactions can be validated by all processing nodes. In a crypto currency blockchain, miners can use the public data to check if a sender account has enough value to process a transaction. In a blockchain running smart contract, miners are able to check any conditions that could be programmed as smart contracts. Encrypting data before storing it on a blockchain may increase confidentiality, but may reduce performance. Storing only a hash of data on-chain and keeping the raw data off-chain improve confidentiality and performance, but partly undermines the distinctive benefit of blockchains in providing distributed trust. Transparency
is in tension with commercial confidentiality and even if encryption is used. Consortium and private blockchains can provide read access controls, but this does not provide commercial confidentiality between the competitors. The main trade-off is between the benefits of sharing data within the
group of collaborators (visibility) and retaining confidentiality towards competitors where needed.

E. Data integrity

The data integrity of transaction history is required. Data integrity of the historical transactions is key for creating provenance, which can be used to track the physical assets through changes in ownership and handling. Using blockchain to achieve integrity may be expensive compared to other persistence mechanisms. There are mechanisms available to prove the origin of data, like hashing technology, and to cryptographically sign data. Architecture with existing tracking mechanism may be less benefited from the provenance information added by using a blockchain.

F. Data immutability

The third-party service providers are not always trustworthy, and a significant benefit of blockchain systems may be in a strong support. The linking of blocks in a chain of cryptographic hashes supports a kind of historical transactions. Data in blockchain cannot be changed easily because it is continually replicated across many different locations and organizations; attempts to change it in one location will be interpreted as an attack on integrity by other participants, and is rejected. This is a good thing but can even cause problems. In real world problems may arise such as disputed transactions, incorrect addresses, exposure or loss of private keys, data-entry errors, unexpected changes to assets tokenized on the blockchain or if a court orders illegal content to be removed from the blockchain. The concerns over the transactions need to be considered during the system design. The immutability of blockchain makes it less adaptable than that of the conventional technologies controlled by third party which also supports rollback.

G. High performance

Since blockchains are currently not highly scalable, hence high performance is not necessarily an inherent limitation, and may be overcome in near future. Consortium and private blockchains with careful design and performance tuning has better performance compared with public blockchain. Blockchain is not suitable for Big Data due to large volumes of data and high velocity data. This is one of the limitations of blockchain. The current work is to store the large amount of data off-chain which avoids duplication of the data to all the connected peers.

V. CONCLUSIONS

Blockchain is an effective solution for the old consensus problem. Using cryptography (hashes

and digital signatures) and a system that rewards participants, the winner of a cryptographic lottery reaps the rewards while it also ensures the validity of the ledger. Blockchain is not a universal solution to any problem having to do with transaction verification and security. The implementation should be adopted only after careful study of the requirements of the application. The impact of the blockchain is disruptive, and the consequences of its widespread adoption are still unknown to the society. Blockchain is at its early stage of its research and development. Researchers in the domain of security and Cryptography have come forward to its newer highs. Blockchain will be at a great help for the Financial and Non Financial sectors. It will overcome to the issues of reliability, security and shared knowledge at the same time. It is one of the most attractive technologies since its inception. We thus conclude that there are ample of opportunities of research in this area and there is also an urgency to explore and seek for betterment just by minimizing the flaws and by enhancing its efficiency distribution.

REFERENCES

[1] Ehsani and Farzam, "Blockchain in Finance: From Buzzword to Watchword," CoinDesk (News), 22 December, 2016.

[2] Linux Foundation unites the Industry leaders to advance Blockchain Technology, 2016..

[3] Open Source Blockchain Effort for the Enterprise Elects Leadership Positions and Gains New Investments, 2016.

[4] Zhao et al., "Financial Innovation," 2-28, 2016.

[5] S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[6] P. Bailis, A. Narayanan, A. Miller, and S.Han, "Research for practice: Cryptocurrencies, blockchains, and smart contracts; hardware for deep learning," Commun. ACM, vol. 60, no. 5, pp. 48–51, 2017.

[7] D. Puthal, S. P. Mohanty, P. Nanda, and U. Choppali, "Building security perimeters to protect network systems against cyber threats," IEEE Consum. Electron. Mag., vol. 6, no. 4, pp. 24–27, 2017.

[8] D. Puthal, S. Nepal, R. Ranjan, and J. Chen, "Threats to networking cloud and edge datacenters in the Internet of Things," IEEE Cloud Comput., vol. 3, no. 3, pp. 64–71, 2016.

[9] D. Puthal, R. Ranjan, S. Nepal, and J. Chen, "IoT and big data: An architecture with data flow and security issues," in Proc. Cloud Infrastructures, Services, and IoT Systems for Smart Cities, 2017, pp. 243–252.

[10] BlockGeeks. (2017). 17 blockchain applications that are transforming society. [Online]. Available: https://blockgeeks.com/guides/blockchain-applications/

[11] P. Sundaravadivel, E. Kougianos, S. P. Mohanty, and M. Ganapathiraju, "Everything you wanted to know about smart healthcare," IEEE Consum. Electron. Mag., vol. 7, no. 1, pp. 18–28, 2018.

[12] I. Giechaskiel, C. J. F. Cremers, and K. B. Rasmussen, "On bitcoin security in the presence of broken cryptographic primitives," in Computer Security - ESORICS 2016 - 21st European Symposium on Research in Computer Security, Heraklion, Greece, September 26-30, 2016, Proceedings, Part II, ser. Lecture Notes in Computer Science, I. G. Askoxylakis, S. Ioannidis, S. K. Katsikas, and C. A. Meadows, Eds., vol. 9879. Springer, 2016, pp. 201–222.