Blockchain applications and challenges: An Review

Nitin Kumar,
Student, M.Tec(CS).
U.P.T.U

Himanshu Sharma
Assistant Professor,
Translam Institute of Tech.

Abstract

As we know Blockchain is buzzword nowadays. It is one of the transformational technologies bringing rapid changes in our professional as well as personal lives. Blockchain has brought the IT revolution in the information security and healthcare. In this paper, we have elaborated numerous applications and challenges. Moreover, this paper highlighted the future directions in the blockchain technology.

Keywords: Blockchain, Cryptocurrency, Hyper Ledger, Decentralized platform, Distributed Ledger.

1. Introduction

We are living the digital era, where every service is being available online for the welfare of society as well as every individual. There should be transparency, security and privacy in every daily routine transaction. For that there should be computational and information sharing platform which enables multiple domain to corporate, coordinate and collaborate in a decision making process. Blockchain is the technology that Blockchain has various benefits such as persistency, decentralization and auditability. It has a wide range of applications starting from healthcare, financial services, cryptocurrency, Internet of Things to public and social services. In last few years, we have seen that cryptocurrency has attracted wide attentions from both academia and industry. Everyone is aware about the name Bitcoin that is frequently called the first cryptocurrency has enjoy a enormous success with the capital market reaching 10 billion dollars in 2016 [3]. The blockchain is the core mechanism for the Bitcoin. Blockchain was first proposed in 2008 and implemented in 2009 [4]. Blockchain is considered as a public ledger, in which all committed transactions are stored in the form of chain of blocks. This chain continuously grows when new blocks are appended to it.

2. Blockchain Technology: How does it work?

The blockchain technology can be applicable to any digital asset transaction exchanged online. First, it validates the entries, then provide the privacy through the cryptography and in the last it preserve the records. Electronic commerce is solely tied to the financial institutions serve as the trusted third party which process and arbitrate every electronic transaction. These third parties play an important role in validation, safeguard and preserving the transactions. A convinced proportion of fraud is inevitable in online transactions and that needs intercession by financial transactions. This consequences in high transaction costs that can be decreased by using blockchain technology easily. It also protect each transaction through a digital signature that's sent with the "public key" of the receiver and digitally signed using the "private key" of the sender.

Each transaction is then broadcasted to each and every node in the network and is then recorded in a public ledger after verification. Fig.1 demonstrate the working of blockchain technology for a financial transactions. For example, Abhinav send some money to Vijay, this transaction is represented online as a “block”. This block is broadcast to every party in the network. Those in the network they will approve this transaction’s validity so that this block can be added to the chain and provides an indelible as well as transparent record of transactions. The verifying node have to ensure two things before recording the transaction.

1. Sender should owns the cryptocurrency, through the digital signature verification.
2. Sender should have sufficient cryptocurrency in his/her account before finalizing the transaction.

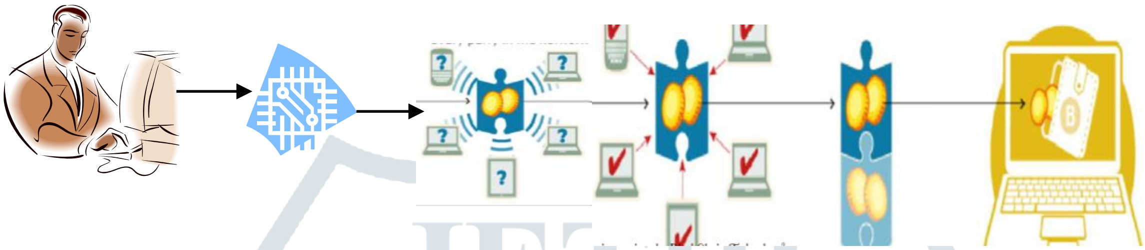

Fig. 1 : Financial transaction through the Blockchain Technology

2.1 **Architecture**

Blockchain is a series of blocks, which holds an inclusive list of transaction records like straight public ledger [5]. Fig. 2 illustrated how blocks are connected with each other. Every block points to the instantly previous block via a reference that is basically a hash value of the earlier block known as a parent block.

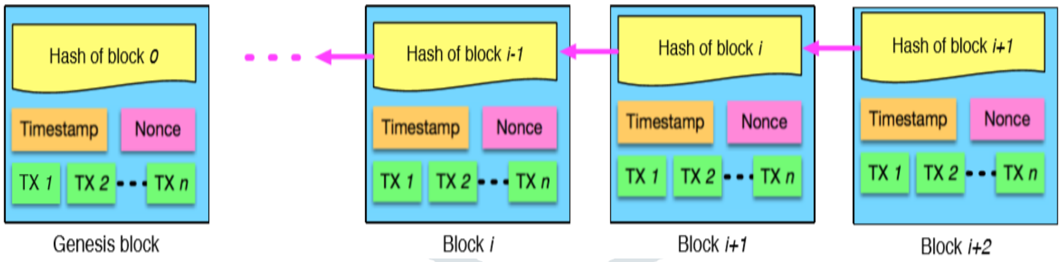

Fig.2 Connected Blocks in Blockchain

2.1 **Block :** A block is an entity of blockchain technology that consists of the block header and the block body as exposed in Fig. 3.In particular, the block header contains :

(i) Block version: indicates which set of block validation rules to follow.

(ii) Parent block hash: contain a hash value that points to the previous block.

(iii) Merkle tree root hash: this hash value indicates to all the transactions in the block.

(iv) Timestamp: store the current timestamp since 1970-01-01T00:00 UTC.

(v) nBits: store the current hashing target.

(vi) Nonce: starts with 0 and increases for every hash calculation.

Header

Block version	02356000
Parent Block Hash	C7gg0d11860n40bd9e7000
Merkle Tree Root	7d11aa54rr8937bb830m81
Timestamp	29k97a43
nBits	30c31b18
Nonce	Se9f0892

Transaction Counter

Tx1.. Tx2 …. Tx'n

Fig.3 : Structure of a block

The block body is composed of a transaction counter and transactions. The maximum number of transactions usually depends on the block size and the size of each transaction. Asymmetric cryptography mechanism is used in blockchain to validate the authentication of transactions [6]. Digital signature is the technique that is used in untrustworthy environment.

2.2 **Digital Signature:** The typical digital signature is the process of authentication that complete in two phases: First, the signing phase and second, the verification phase. Suppose, a user Alice wants to sign a transaction, he first generates a hash value consequent from the transaction. He will apply the encryption on the hash value with his private key and sends to receiver Bob. When he will receive the encrypted hash with the original data, he verify this transaction through the evaluation decrypted by using Alice's public key and the hash value derived from the received data by the same hash function as Alice's. The classic digital signature algorithms used in blockchain s comprise elliptic curve digital signature algorithm (ECDSA) [7].

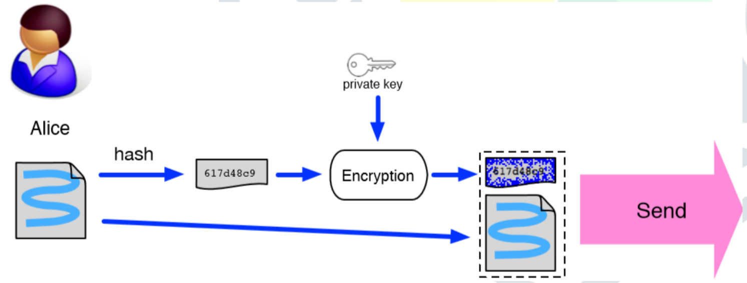

Fig. 4(a) Signing process of Digital Signature

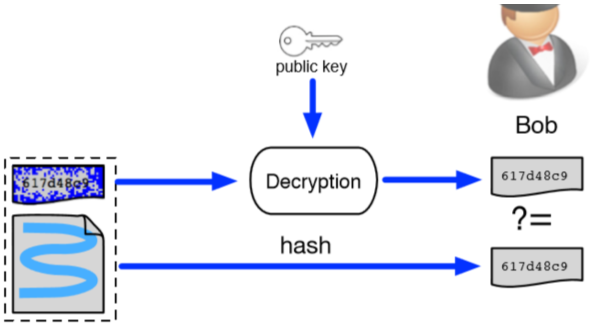

Fig. 4(b) Verification process of Digital Signature

3. Key Charactertics of Blockchain

- **Decentralization: Since every** transaction in the blockchain network can be conducted between any two peer-to-peer (P2P) without the authentication by the central agency. That's why, blockchain has significantly reduced the server costs.
- **Persistency: As** each of the transactions scattering crosswise the network needs to be confirmed and recorded in blocks distributed in the network, that's why it is almost impossible to alter.
- **Anonymity**: Each user can interact with the blockchain network with a generated address.
- **Auditability**: Each transaction can be traced to previous transactions iteratively. It improves the traceability and the transparency of the data stored in the blockchain.

4. Applications of Blockchain

There is a varied of applications of blockchain technology in almost every important domain of the our day-to-day life. Blockchain technology can be applied into many areas including clearing and settlement of financial assets etc. Bitcoin and Ethenum are example that we have seen in last few years. Blockchain has attracted big software companies. Now, Microsoft and IBM are starting Blockchain-as-a-Service.

Blockchain technology has the potential to improve the Internet of Things(IOT) sector.

Zhang et al. [8] has proposed a new IoT E-business model and realize the transaction of smart property based on blockchain and smart contract. In this model, distributed autonomous Corporations(DAC)is adopted as a decentralized transaction entity. People trade with DACs to obtain coins and exchange sensor data without any third party.

One of typical blockchain applications in public services is the land registration[6],in which the land information such as the physical status and related rights can be registered and publicized on blockchains. Besides, blockchains can be used in green energy, education, healthcare and music industry easily to provide the privacy.

5. Challenges

5.1 Scalability

As day by day amount of trasactions are increasing, it will be not easy for the blockchain to store and validate these transaction. As there is some restriction of the block size and the time interval to generate the new block, the blockchain can only process 7 trasaction/second and can't handle real-time business transaction. So, scalability problem is a big challenge.

5.2 Selfish mining

Blockchain is vulnerable to attacks of colluding selfish miners. Generally it is influenced that nodes with over 51% computing power can reverse the blockchain and reverse the happened transaction.

5.3 Privacy Leakage

Blockchain is generally considered a safe place to store the transaction as a "public ledger". However, it is observed by many researchers that blockchain can't give the guarantee of transactional privacy because the values of all transaction and public key are publically available. Multiple methods have been proposed to improve the anonymity of blockchain. In [10], zero-knowledge proof is used. Miners do not have to validate a transaction with digital signature but to validate coins belong to a list of valid coins.

6. Conclusion

Nowadays, Blockchain is well known name for its decentralized infrastructure and peer-to-peer nature. However, many researches has focused on blockchain for Bitcoin and financial purpose. But blockchain can be applied to a diversity of field far beyond Bitcoin. In this paper, we tried to find out some important applications in the fastest growing sectors of world economy. We also covered the major challenges that are coming during the implementation of blockchain in our public and private sectors. In future, we are planning to take a in-depth survey on smart contract and impact of artificial intelligence.

References

1. Ibm blockchain (2016), http://www.ibm.com/blockchain/
2. Microsoft azure: Blockchain as a service (2016), https://azure.microsoft. com/en-us/solutions/blockchain/
3. State of blockchain q1 2016: **Blockchain funding overtakes bitcoin** (2016), http: //www.coindesk.com/state-of-blockchain-q1-2016/
4. Nakamoto, S.: **Bitcoin: A peer-to-peer electronic cash system** (2008), https:// bitcoin.org/bitcoin.pdf
5. **Lee Kuo Chuen, D. (ed.):** Handbook of Digital Currency. Elsevier, 1 edn. (2015), http://EconPapers.repec.org/RePEc:eee:monogr: 9780128021170
6. **NRI: Survey on blockchain technologies and related services. Tech. rep. (2015)**
7. **Johnson,D.,Menezes,A.,Vanstone,S.:**The elliptic curve digital signature algorithm (ecdsa). International Journal of Information Security 1(1), 36–63 (2001).
8. **Zhang, Y., Wen, J.:** An iot electric business model based on the protocol of bitcoin. In: Proceedings of 18th International Conference on Intelligence in Next Generation Networks (ICIN). pp. 184–191. Paris, France (2015)
9. **Crypto-currency market capitalizations** (2017), https://coinmarketcap.com
10. **Miers, I., Garman, C., Green, M., Rubin, A.D.:** Zerocoin: Anonymous distributed ecash from bitcoin.In:ProceedingsofIEEESymposiumSecurityandPrivacy(SP).pp. 397–411. Berkeley, CA, USA (2013)
11. Akins, B.W., Chapman, J.L., Gordon, J.M.: **A whole new world: Income tax considerations of the bitcoin economy** (2013), https://ssrn.com/abstract= 2394738
12. Zibin Zheng, Shaoan Xie, **Blockchain Challenges and Opportunities: A Survey**, Int. J. Web and Grid Services: Inderscience, 2017, 1-25
13. Zheng, Z., Xie, S., Dai, H., Chen, X.,Wang, H.: **An overview of blockchain technology: Architecture, consensus, and future trends**. In: Proceedings of the 2017 IEEE BigData Congress. pp. 557–564. Honolulu, Hawaii, USA (2017)
14. Zyskind, G., Nathan, O., et al.: **Decentralizing privacy: Using blockchain to protect personal data**. In: Security and Privacy Workshops (SPW), 2015 IEEE. pp. 180–184. IEEE (2015)