Block Chain Technology

Authors: Akash Singh, Ganesh Sawant,

H. O. D: Mr. S. D. Sanap , sanapsd@gmail.com

Staff member: Mrs.Vaishali Chate, chatevaishali8@gmail.com

GOVERNMENT POLYTECHNIC, THANE

Abstract: Blockchain, the foundation of Bitcoin, has received extensive attentions recently. Blockchain serves as an immutable ledger which allows transactions take place in a decentralized manner. Blockchain-based applications are springing up, covering numerous fields including financial services, reputation system and Internet of Things (IoT), and so on. However, there are still many challenges of blockchain technology such as scalability and security problems waiting to be overcome. This paper presents a comprehensive overview on blockchain technology. We provide an overview of blockchain architechture firstly and compare some typical consensus algorithms used in different blockchains. Furthermore, technical challenges and recent advances are briefly listed. We also lay out possiblefuture trends for blockchain.

Index: Block chain Technology, Fundamentals of blockchain technology, Characteristics, Uses, Future of blockchain technology, Conclusion

1. Introduction

Nowadays cryptocurrency has become a buzzword in both industry and academia. As one of the most successful crypto currency, Bitcoin has enjoyed a huge success with its capital market reaching 10 billion dollars in 2016. With a specially designed data storage structure, transactions in Bitcoin network could happen without any third party and the core technology to build Bitcoin is blockchain, which was first proposed in 2008 and implemented in 2009. Blockchain could be regarded as a public ledger and all committed transactions are stored in a list of blocks. This chain grows as new blocks are appended to it continuously. Asymmetric cryptography and distributed consensus algorithms have been implemented for user security and ledger consistency. The blockchain technology generally has key characteristics of decentralization, persistency, anonymity and auditability. With these traits, blockchain can greatly save the cost and improve the efficiency.

Blockchain could be regarded as a public ledger and all committed transactions are stored

in a list of blocks. This chain grows as new blocks are appended to it continuously. Asymmetric cryptography and distributed consensus algorithms have been implemented for user security and ledger consistency. The blockchain technology generally has key characteristics of decentralization, persistency, anonymity and auditability. With these traits, blockchain can greatly save the cost and improve the efficiency.

2.Technology Fundamentals of Blockchain:

This section briefly describes the fundamentals of the technology behind the Blockchain. A Blockchain comprises of two different components, as follows:

2.1. Transaction: A transaction, in a Blockchain, represents the action triggered by the participant.

2.2. Block: A block, in a Blockchain, is a collection of data recording the transaction and other associated details such as the correct sequence, timestamp of creation, etc.

2.3 Digital Signature:

Each user owns a pair of private key and public key. The private key that shall be kept in confidentiality is used to sign the transactions. The digital signed transactions are broadcasted throughout the whole network. The typical digital signature is involved with two phases: *signing phase* and *verification phase*. For instance, an user Alice wants to send another user Bob a message.

(1) In the signing phase, Alice encrypts her data with her private key and sends Bob the encrypted result and original data.

(2) In the verification phase, Bob validates the value with Alice's public key. In that way, Bob could easily check if the data has been tampered or not.

The typical digital signature algorithm used in blockchains is the elliptic curve digital signature algorithm (ECDSA).

The Blockchain can either be public or private, depending on the scope of its use. A public Blockchain enables all the users with read and write permissions such as in Bitcoin, access to it. However, there are some public Blockchains that limit the access to only either to read or to write. On the contrary, a private Blockchain limits the access to selected trusted participants only, with the aim to keep the users' details concealed. This is particularly pertinent amongst governmental institutions and allied sister concerns or their subsidies thereof.

One of the major benefits of the Blockchain is that it and its implementation technology is public. Each participating entities possesses an updated complete record of the transactions and the associated blocks. Thus the data remains unaltered, as any changes will be publicly verifiable. However, the data in the blocks are

encrypted by a private key and hence cannot be interpreted by everyone.

- Another major advantage of the Blockchain technology is that it is decentralized. It is decentralized in the sense that:
  - There is no single device that stores the data (transactions and associated blocks), rather they are distributed among the participants throughout the network supporting the Blockchain.
  - The transactions are not subject to approval of any single authority or have to abide by a set of specific rules, thus involving substantial trust as to reach a consensus.
  - The overall security of a Blockchain eco-system is another advantage. The system only allows new blocks to be appended. Since the previous blocks are public and distributed, they cannot be altered or revised.

For a new transaction to be added to the existing chain, it has to be validated by all the participants of the relevant Blockchain eco-system. For such a validation and verification process, the participants must apply a specific algorithm. The relevant Blockchain eco-system defines what is perceived as "valid", which may vary from one eco-system to another. A number of transactions, thus approved by the validation and verification process, are bundled together in a block. The newly prepared block is then communicated to all other participating nodes to be appended to the existing chain of blocks.

Each succeeding block comprises a hash, a unique digital fingerprint, of the preceding one.

3.0 Key Characteristics of Blockchain

In summary, blockchain has following key characteristics.

- **Decentralization.** In conventional centralized transaction systems, each transaction needs to be validated through the central trusted agency (e.g., the central bank), inevitably resulting to the cost and the performance bottlenecks at the central servers. Contrast to the centralized mode, third party is no longer needed in blockchain. Consensus algorithms in blockchain are used to maintain data consistency in distributed network.
- **Persistency.** Transactions can be validated quickly and invalid transactions would not be admitted by honest miners. It is nearly impossible to delete or rollback transactions once they are included in the blockchain. Blocks

that contain invalid transactions could be discovered immediately.

- **Anonymity**. Each user can interact with the blockchain with a generated address, which does not reveal the real identity of the user. Note that blockchain cannot guarantee the perfect privacy preservation due to the intrinsic constraint.
- **Auditability.** Bitcoin blockchain stores data about user balances based on the Unspent Transaction Output (UTXO) model Any transaction has to refer to some previous unspent transactions. Once the current transaction is recorded into the blockchain, the state of those referred unspent transactions switch from unspent to spent. So transactions could be easily verified and tracked.

4. Use of Blockchain beyond Cryptocurrency

Although the Internet is a great tool to aid every sphere of the modern digital life, it is still highly flawed in terms of the lack of security and privacy, especially when it comes to FinTech and E-commerce. Blockchain, the technology behind cryto-currency, brought forth a new revolution by providing a mechanism for Peer-to-Peer (P2P) transactions without the need for any intermediary body such as the existing commercial bank. BC validates all the transactions and preserves a permanent record of them while making sure that any identification related information of the users are kept incognito. Thus all the personal information of the users are sequestered while substantiating all the transactions. This is achieved by reconciling mass collaboration by cumulating all the transactions in a computer code based digital ledger. Thus, by applying Blockchain or similar crypto-currency techniques, the users neither need to trust each other nor do they need an intermediator; rather the trust is manifested within the decentralized network system itself. Blockchain thus appears to be the ideal "Trust Machine" paradigm.

Uses of Blockchain apart from banking:

- **Healthcare:** Each of us has a record of all the ailments and clinical procedures that we have gone through. Generally, when we approach a doctor we only provide basic details of the disease which we are currently suffering through. Hence doctors don't usually have all the records that they might need to treat our illness better. These records may also contain information about any kind of allergies that we have or any previous treatment that might be relevant to our current medical condition. Blockchain can help create records of patients' treatments and provide doctors with relevant information by bringing the entire information online. Since data would be encrypted it is much secure

than directly storing the data over a cloud storage.

- **Identity Management:** Governments across the world maintain a record of the identity of their citizens. These may include social security numbers, passport, PAN Card details etc. Managing a record of each ID is a complex procedure and it is also unsafe to keep this data online. Blockchain can be a great alternative for traditional storage as it provides a ledger system that can be used to record any size of information. Since it is encrypted it will obviously be safer than storing the data over a hard drive or in traditional filing systems. It will be helpful for both the government and people as either party can easily gain access to the required information without any hassle.
- **Voting:** Voting here can be used in either sense whether we talk about voting for elections or shareholders voting. In either of the case, it is a possibility that the actual data is tampered or manipulated by exploiting a vulnerability in the system. On the contrary, if blockchain is used to manage the same information we can create a much safer mechanism to manage the same task. Since in blockchain we use smart contracts the data would be immutable and the person cannot change his decision once he has given the vote.

5. The Future of Blockchain

According to the Gartner Hype Cycle for Emerging Technologies 2017, shown in Figure 2, below, Blockchain still remains in the region of "Peak of Inflated Expectation" with forecast to reach plateau in "five to ten years". However, this technology is shown going downhill into the region of the "Trough of Disillusionment". Because of the wide adoption of the Blockchain in a wide range of applications beyond cryptocurrency, the authors of this paper are forecasting a shift in classification from "five to ten years" to "two to five years" to reach maturation. Blockchain possesses a great potential in empowering the citizens of the developing countries if widely adopted by e-governance applications for identity management, asset ownership transfer of precious commodities such as gold, silver and diamond, healthcare and other commercial uses as well as in financial inclusion. However, this will strongly depend on national political decisions.

6.Conclussion: . Gartner Hype Cycle, 2017 [11] The application of the Blockchain concept and technology has grown beyond its use for Bitcoin generation and transactions. The properties of its security, privacy, traceability, inherent data provenance and time-stamping has seen its adoption

beyond its initial application areas. The Blockchain itself and its variants are now used to secure any type of transactions, whether it be human-to-human communications or machine-to-machine. Its adoption appears to be secure especially with the global emergence of the Internet-of-Things. Its decentralized application across the already established global Internet is also very appealing in terms of ensuring data redundancy and hence survivability. The Blockchain has been especially identified to be suitable in developing nations where ensuring trust is of a major concern. Thus the invention of the Blockchain can be seen to be a vital and much needed additional component of the Internet that was lacking in security and trust before. BC technology still has not reached its maturity with a prediction of five years as novel applications continue to be implemented globally.

7.References :

[1] Nir Kshetri, "Can Blockchain Strengthen the Internet of Things?," IT Professional, vol. 19, no. 4, pp. 68 - 72, May 2017, Available: http://ieeexplore.ieee.org/document/8012302/

[2] Mahdi H. Miraz, "Blockchain: Technology Fundamentals of the Trust Machine," Machine Lawyering, Chinese University of Hong Kong, 23rd December 2017, Available: http://dx.doi.org//10.13140/RG.2.2.22541.64480/2

[3] Don Tapscott and Alex Tapscott, Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World, 1st ed. New York, USA: Penguin Publishing Group, 2016.

[4] Maaruf Ali and Mahdi H Miraz, "Cloud Computing Applications," in Proceedings of the International Conference on Cloud Computing and eGovernance - ICCCEG 2013, Internet City, Dubai, United Arab Emirates, 2013, pp. 1-8, Available: http://www.edlib.asdf.res.in/2013/iccceg/paper001.pdf

[5] Maaruf Ali and Mahdi H. Miraz, "Recent Advances in Cloud Computing Applications and Services," International Journal on Cloud Computing (IJCC), vol. 1, no. 1, pp. 1-12, February 2014, Available: http://asdfjournals.com/ijcc/ijcc-issues/ijcc-v1i1y2014/ijcc-001html-v1i1y2014/

[6] What is Blockchain Technology? –CoinDesk https://www.coindesk.com/information/what-is-blockchain-technolog