International Journal of Industrial Engineering & Production Research June 2020 Vol. 31, No. 2: 309-315
DOI: 10.22068/ijiepr.31.2.309

RESEARCH PAPER

BlockChain: Properties, Application, and Bitcoin Case study.

Harika Devi Kotha[1]*,V Mnssvkr Gupta[2]

Received 18 April 2020; Revised 28 April 2020; Accepted 3 May 2020; Published online 30 June 2020

ABSTRACT
Blockchain is a decentralized distributed network that allows Peer-to-Peer (P2P) communication among the users. As the name suggests, it deals with a group of records called blocks. We are in an era where it is important to maintain the integrity of data as well as to fasten the process of the transaction. Blockchain helps perform these by maintaining the timestamp on blocks and the time required for a transaction can be shortened by eliminating the need of the third party during the process of the transaction. Bitcoin and Smart contract are two major applications based on blockchain technology. Bitcoin is the first application that was developed on blockchain technology and is a popularly known cryptocurrency. Satoshi Nakamoto is the so-called creator of bitcoin and its development [1]. Smart contract was defined by Szabo as a "set of promises, specified in digital form, including protocols within which the parties perform on these promises [2]. This paper aims to present a detailed overview of blockchain and its applications followed by a case study on bitcoin.

KEYWORDS: *Blockchain; bitcoin; smart contract; crypto-currency; protocol.*

1. Introduction

The term blockchain deals with a group of records generally called as blocks [3]. Each user in the blockchain network will have the entire list, which is called as the *shared ledger*. Each block in the ledger contains data and hash for that data. Hash is a cryptographic technique that ensures data security, i.e., helps avoid unauthorized data access. As in a two-way linked list, each block has a logical connection to the next and previous blocks, meaning that, in each block, hash of its own block and hash of its previous block will be maintained. The first block in the shared ledger is called as *genesis block* or *root block.*

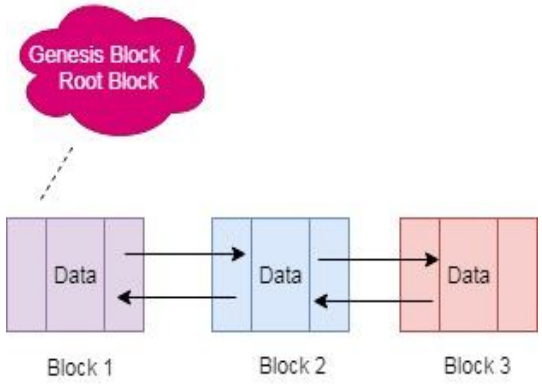

Fig. 1. Blockchain

As mentioned earlier, each user will have a shared ledger. Blockchain uses mesh topology within the group, ie., each user will maintain a point-to-point connection to all other users in the group, which helps a P2P communication among the users within the network, as shown.

* **Corresponding author:** ***Harika Devi Kotha***
ecmharika@ifheindia.org

1. *Assistant Professor, Department of ECE, IFHE-FST, Hyderabad- 501203, India.*
2. *Assistant Professor, Department of CSE, SRKR Engineering College, Bhimavaram, India.*

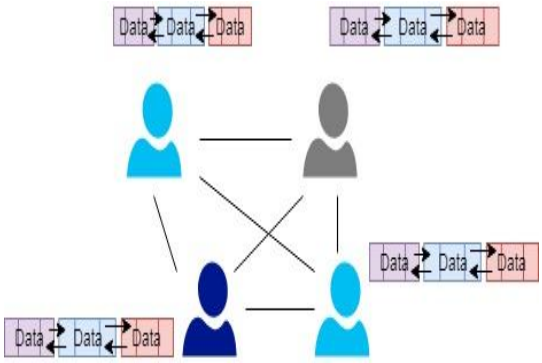

Fig. 2. how a Blockchain network looks like

Whenever a new block is created, it will be appended to the end of the shared ledger. Blockchain technology maintains timestamp in order to avoid tampering of data.

The mainly used cryptographic algorithms are SHA-256. The main feature of SHA-256 is irrespective of the message (input block) size, and the encrypted output is 256bit length. Even small changes in input (e.g., lower case to upper case of an alphabet) change the hash generated.

Along with the **data**, each block in the blockchain network contains the following, which is shown in Figure 2.

- Index, which is nothing but a block number.
- timestamp, which gives details of the time when a block is created.
- previous block hash and its respective hash [4].

2. Blockchain

2.1. Building a blockchain

1. Select the application (use case) for which the blockchain network has to be developed [6].
2. Select a platform (like Corda, credits, etc.) for developing blockchain
3. Create a genesis block.
4. Use hashing algorithms to generate the hash for the data
5. whenever a new transaction takes place, perform the following steps:
    - Allocate an index number
    - Calculate the hash for the data
    - Connect the block to the end of the network by pointing to the hash of the previous block.

2.2. Properties of blockchain

- Blockchain uses **decentralized** network configuration [5]. Therefore, at any point in time, anyone in the blockchain network can interact (in other words, perform transactions) with others without the third-party intervention.
- Another most important feature of blockchain is **transparency.** It is claimed that only the transactions in the network can be seen and, also, the identity of the person is kept secure. This is achieved by displaying the encrypted data instead of the person's identity.
- The data in the blockchain network is **immutable**. Since blockchain maintains the shared ledger, one cannot tamper the data in the network.

2.3. SHA 256

Secure Hash Algorithm (SHA) 256 is a family of cryptographic hash functions [7]. It is a variant of SHA 2. SHA 256 takes 32-bit word inputs and produces 256-bit output, commonly called Hash. The main advantage of SHA 256 is a small change in input changes the generated hash. Different operations involved in the algorithm are given below:

AND, XOR, ROTATION, MOD 2^{32} addition, OR, SHR. The following table shows the SHA 256 output for various inputs:

Tab. 1. SHA 256 hash for various inputs

S.No	Message	SHA 256 Hash
1	harika	6C12BDB955161113E8B04CDC20D975A8457949E0DADA8CDBEA38501AFFD4BB92
2	Harika	A9F76F9706752C980AF2BC81DF6BB5A97B20F07E88DC265CD7EBFDA2D249DFB8
3	hai Harika how are you	BE2D85BE3DA2E59A5FD12DA8601910E6A593B3758D1D52D8ADC496742F275F1E
4	Ha	72AA80BF1AC4EEF0263917C350D8941A1C3F90B3B50D1232B52E6CEDA51D5

		3D4
5	blockchain applications	C6D98EE93E0E33AB1777B8BB5249C80D27BA7A8E26A7959BED2D1F9F37451480
6	block-chain applications	DD41149CEBB4762F5804EAC5613B4B51E1C394CA869B488935C51DB5406020D2

From the above table, it is understood that even a small change, i.e., Inputs 1 and 2, in the hash generated is different. In addition, from Inputs 3 and 4, it is understood that irrespective of the message, the output is always of 256bit length.

2.4. Smart contracts

Smart contract is a protocol that is designed to verify or enforce the negotiation of a contract [8]. This allows performing the transactions without involving the third party. These transactions can be tracked and are irreversible in nature., ie., we have to properly verify the integrity of the transaction before adding it to the blockchain network. Because of smart contracts, transaction costs can be minimized.

2.5. Types of blockchain

The following are the types of blockchain:

- Public blockchain,
- Private Blockchain,
- Consortium blockchain.

Public blockchains are open in nature, i.e., any person can join the network irrespective of location, nationality, etc. It puts the full decentralized nature on display. It allows anyone to act as a user, miner, developer, etc. One of the problems of this type is its difficulty to identify whether a transaction is valid or not.

Unlike Public blockchain, **Private blockchain** needs permissions to join a particular blockchain network. Thus, it can be mentioned that this type is somewhat centralized in nature when compared to the public blockchain.

Lastly, **Consortuim blockchains** are of similar properties as private blockchain with minor differences. The difference is that the consortium blockchain is governed by a group rather than by a single entity [9].

3. Applications

Due to the advantages of blockchain technology, it can be applied to various fields. Therefore, we would like to list a few areas where blockchain technology can be used.

3.1. In voting system :

Election manipulation or vote rigging is a major concern in elections. Given that blockchain is decentralized, immutable, and transparent, by means of blockchain technology, one can implement a highly secured voting system. Whenever a voter gives their vote, it can be added as a block to the network. Since the blockchain network is immutable and tamper-proof, one can maintain transparency in the voting system [10].

3.2. In supply-chain management

In the supply chain, blockchain technology can be used to maintain the details of a product from its origin until it reaches the user. At each level, the information can be added as a node and saved. By doing this, it becomes easy to identify where exactly a fault occurs in the case needed. Wallmart is one of the best examples that brought transparency to the food supply chain [11] using block technology. In doing so, one can promote customer/user trust.

3.3. Internet of things (IoT)

A network where various things (devices) can communicate (transfer of information) using a set of protocols and have the ability to take action is generally called "Internet of Things" [12][13][14]. Security and scalability are the main concerns of IoT. As blockchain is using highly secured cryptographic algorithms, it is tamper-proof and, by means of blockchain technology, we can attempt to improve these aspects of IoT [15].

3.4. In agriculture

Combing IoT with blockchain, we can achieve good results in the field of agriculture. The application of sensors can get the parameters of soil and save them in the blockchain network. Since the data are transparent to the farmers, one can decide what minerals the soil is lacking; thus, instead of using powerful fertilizers, farmers can use those fertilizers that the land and crop really require.

In the case of crop yield, blockchain technology can be used for crop insurance [16],[17]. Since it

is a shared ledger and is transparent, the farmer will no longer be waiting for insurance money in case of loss due to weather-related incidents, floods, etc.

3.5. In healthcare

Record keeping is very important in the healthcare domain. There will be so many things like patient previous health data, patient lab reports, patient present situation, and what type or which medicines are prescribed for the patient in the current scenario, etc. that can be made as blocks and can be shared between the doctor and patient such that doctor-patient interactions will be improved.

Similar to record keeping, blockchain enchases the security and control of healthcare transactions. As claimed, the patient payment records can be maintained securely [18].

3.6. In logistics

Combining IoT sensors with blockchain technology, we can save the billing information, goods information, from seller endpoint to retailer. All related information will be saved in blocks and can be tied together to have a strong network.

Apart from the above-discussed applications, Blockchain can be implemented in various fields where security and transparency of data are indeed required.

4. Bitcoin: Case Study

Bitcoin is one of the most popular cryptocurrencies that was introduced by Satoshi Nakamoto in his whitepaper "bitcoin: a peer-to-peer electronic cash system". Bitcoin is the first commercial application of blockchain technology, and the term bitcoin was firstly introduced by the anonymous author Satoshi Nakamoto[19], where he defined bitcoin as an "electronic cash and the transactions can be done end to end without the involvement of a third party". Bitcoin uses a peer-to-peer communication and it is decentralized in nature. Bitcoin is widely accepted as the most popular cryptocurrency. Apart from bitcoin, there are different cryptocurrencies including Ethereum, etc.

In this case study, the focus is to discuss the security concerns about bitcoin. Even though bitcoin uses very secured cryptographic methods, numerous attacks have occurred on different aspects of bitcoin. One such attack is ***Double Spending***, which means that one will spend the same cryptocurrency (bitcoin) in two different transactions.

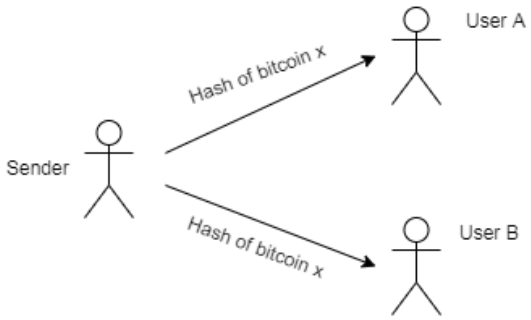

Fig. 3. Double spending

On November 2013, it was discovered that the ***GHash.io*** mining pool appeared to be engaging in repeated payment fraud against BitCoin Dice, a gambling site [21][22].

There are so many forms of double spending attack and one such attack is *Finney attack* [23][24]. In this type of attack, the attacker will initially pre-mine the network and will try to perform the transaction with those details he obtained during private mining. It is implied that he will create two transactions –for the victim and for him; once the transaction is done, he will release the pre-mined block into the network, which then becomes invalidated. There are so many other types of attacks like Vector 76 or one-confirmation attack, > 50% hashpower or Goldfinger, fork after withholding (FAW) attack, Block withholding [25][26][27][28][29], etc.

To avoid these types of attacks, one has to wait until he/she receives validation from other users in the network. Then, only these types of attacks can be minimized. Moreover, these types of security issues in trading can be reduced if an extra security concern like getting help from a third party as in ***Escrow service*** [30] is considered. When combined with multi-

signature, such services can ensure better security.

Furthermore, there is a privacy-related protocol called ***Zero-coin*** as proposed by Matthew D Green et al. [31] and it enhances the privacy issue (attacks on) of bitcoin. The Zero-coin is considered to be an extension to bitcoin and is designed to improve the anonymity of bitcoin transactions. Zero-coin has a coin mixing capacity which is built on the protocol [32].

In addition bitcoin, there are so many cryptocurrencies in today's' market, some of which include Ethereum (Ether), Mastercoin (MSC), Counterparty (XCP), Zcash, Primecoin, Litecoin, peercoin, etc. [33]. Today, there are approximately 1146 different cryptocurrencies in action [34], among which Bitcoin and Ethereum enjoy the highest popularity.

5. Conclusion

Characterized by immutability, smart contracts, and high security, Blockchain technology can be implemented in various fields. This paper presents a brief overview of blockchain properties and its applications and a case study on security aspects of bitcoin. It cannot be stressed enough that cryptocurrencies are only one of the applications of blockchain. From the case study on bitcoin, after observing so many robust features of bitcoin such as proof-of-work, there are still various security attacks occurring like simple packet sniffing to double spending. To enhance the security of bitcoin, ***Escrow service*** with multi-signature concepts should be considered. Therefore, it can be claimed that there is a wide research gap concerning bitcoin security and one can work to improve the security and privacy aspects of Bitcoin.

References

[1] Wikipedia contributors. (2019, May 2). Satoshi Nakamoto. In Wikipedia, The Free Encyclopedia. (2019), from https://en.wikipedia.org/w/index.php?title=Satoshi_Nakamoto&oldid=895178150.

[2] Shuai Wang et.al., " Blockchain-Enabled Smart Contracts: Architecture,Applications, and Future Trends ", IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS: SYSTEMS, (2019), IEEE.

[3] Wikipedia contributors. Blockchain. In Wikipedia, The Free Encyclopedia. (2019). from https://en.wikipedia.org/w/index.php?title=Blockchain&oldid=897623168.

[4] Sylvain Saurel, " Create your own Blockchain in 30 minutes" ,medium.com, (2018) from https://medium.com/@ssaurel/create-your-own-blockchain-in-30-minutes-dbde3293b390.

[5] Ameer Rosic," What is Blockchain Technology? A Step-by-Step Guide For Beginners, Blockgeeks, (2016) fromhttps://blockgeeks.com/guides/what-is-blockchain-technology/.

[6] Rohas Nagpal, " #8 Steps to Build a Blockchain Solution ", entrepreneur India, (2017), from https://www.entrepreneur.com/article/300077.

[7] Wikipedia contributors. Secure Hash Algorithms. In Wikipedia, The Free Encyclopedia. (2019), from https://en.wikipedia.org/w/index.php?title=Secure_Hash_Algorithms&oldid=924662207.

[8] Wikipedia contributors. Smart contract. In Wikipedia, The Free Encyclopedia. (2019), from https://en.wikipedia.org/w/index.php?title=Smart_contract&oldid=923105708.

[9] Technology, "What Different Types of Blockchains are There?",https://dragonchain.com (2019), fromhttps://dragonchain.com/blog/differences-between-public-private-blockchains/.

[10] LUKE FORTNEYet.al., investopedia," Blockchain Explained ", (2019), from https://www.investopedia.com/terms/b/blockchain.asp.

[11] Hyperledger, , " Case Study:How Walmart brought unprecedented transparency to the food supply chain with Hyperledger Fabric", from https://www.hyperledger.org/resources/publications/walmart-case-study.

[12] Harika devi kotha et.al., " IoT Application, a Survey" , International Journal of Engineering and Technology- UAE,volume Vol. 7, Nos. 2.7, (2018), pp. 891-896.

[13] Harika devi kotha et.al.," An Iot Based Solution For Health Monitoring Using A Body-Worn Sensor Enabled Device" Journal of Advaced Research in Dynamical & Control Systems, Vol. 10, 09-Special Issue, (2018), pp. 646-651.

[14] Harika devi kotha et.al," An Overview of Internet of Things", Journal of Advaced Research in Dynamical & Control Systems, Vol. 10, 09-Special Issue, (2018), pp. 659-665.

[15] Ahmed Banafa, " How to Secure the Internet of Things (IoT) with Blockchain", dafloq.com, (2017), from https://datafloq.com/read/securing-internet-of-things-iot-with-blockchain/2228.

[16] LeewayHertz, " How will Blockchain Agriculture revolutionize the Food Supply from farm to plate?" hackernoon.com, (2019), from https://hackernoon.com/how-will-blockchain-agriculture-revolutionize-the-food-supply-from-farm-to-plate-f8fe488d9bae.

[17] Akash Takyar ," Blockchain in Agriculture – Improving Agricultural Techniques", https://www.leewayhertz.com, from https://www.leewayhertz.com/blockchain-in-agriculture/.

[18] Bryan Weinberg, " 10 Major Real Use Cases of Blockchain in Healthcare ", openledger insights, (2019), from https://openledger.info/insights/blockchain-healthcare-use-cases/.

[19] Satoshi Nakamoto, " Bitcoin: A Peer-to-Peer Electronic Cash System", (2008) from https://bitcoin.org/bitcoin.pdf.

[20] Andrew LR and Douglas AO (2018) Bitcoin Investigations: Evolving Methodologies and Case Studies. J Forensic Res 9: 420. DOI: 10.4172/2157-7145.1000420.

[21] Irreversible Transactions from https://en.bitcoin.it/wiki/Irreversible_Transactions.

[22] Bitcoin Forum from BitcoinTalk Thread - GHash.IO and double-spending against BetCoin Dice.

[23] H. Finney, "Best practice for fast transaction acceptance how high is the risk?" Available: https:// bitcointalk.org/ index.php?topic=3441.msg48384#msg48384 (2011).

[24] Mauro counti et.al., " A Survey on Security and Privacy Issues of Bitcoin", IEEE communications surveys & Tutorials, Vol, 201, No. 4, (2018).

[25] J. A. Kroll, I. C. Davey, and E. W. Felten, "The economics of bitcoin mining, or bitcoin in the presence of adversaries," (2013).

[26] Vector67, "Fake bitcoins?" Available: https:// bitcointalk.org/ index.php?topic=36788.msg463391#msg463391, (2011).

[27] J. A. Kroll, I. C. Davey, and E. W. Felten, "The economics of bitcoin mining, or bitcoin in the presence of adversaries," (2013).

[28] M. Rosenfeld, "Analysis of bitcoin pooled mining reward systems," CoRR, vol. abs/1112.4980, (2011).

[29] S. Bag, S. Ruj, and K. Sakurai, "Bitcoin block withholding attack : Analysis and mitigation," IEEE Transactions on Information Forensics and Security, No. 99, (2016), pp. 1-12.

[30] Creative Commons Attribution 3.0 , "Secure Trading" , source : https://en.bitcoin.it/wiki/Secure_Trading , 4 (2017).

[31] Matthew D. Green [@matthew_d_green] "We designed a new version of Zerocoin that reduces proof sizes by 98% and allows for direct anonymous payments that hide payment amount" *(Tweet)*. Retrieved 16 September 2015 – *via* Twitter. *,16 November* (2013).

[32] Wikipedia contributors. Zerocoin protocol. In Wikipedia, The Free Encyclopedia. Retrieved 07: 32, (2020), from https://en.wikipedia.org/w/index.php?title=Zerocoin_protocol&oldid=931858447, 2019, December 21.

[33] Wikipedia contributors. "List of cryptocurrencies" In Wikipedia, The Free Encyclopedia. Retrieved 07:52, January 9, 2020, from https://en.wikipedia.org/w/index.php?title=List_of_cryptocurrencies&oldid=916764976, 2019.

[34] Mauro Conti et.al., " A Survey on Security and Privacy Issues of Bitcoin " , arXiv:1706.00916v3 [cs.CR] (2017).

Follow This Article at The Following Site:

Devi Kotha H, Mnssvkr Gupta2 V. BlockChain : Properties, Application and Bit-coin Case study.. IJIEPR. 2020; 31 (2) :309-315
URL: http://ijiepr.iust.ac.ir/article-1-1056-en.html