Global Journal of Enterprise Information System

DOI: 10.18311/gjeis/2016/15770

Block-Chain: An Evolving Technology

K. Siba*, Tarun and Anuj Prakash

Analytics and Insights, TCS, Bangalore, Karnataka, India;
siba.k@tcs.com, tarun.3@tcs.com, anuj.prakash@tcs.com

Abstract

Now a days, the people are attracting towards the digital currency due to demonetization, rapidly changing world, and global payment options etc. The industries are looking for such a technology which works in digital currency environments with the account of all the transactions. In this paper, we have discussed Blockchain technology, an evolving technology, which provides an assistance to the industries in digital currency environment with the record of each transaction. We have discuss the various types of blockchain with the core concept of hashing algorithm. We have discussed the application of blockchain in different industries and how it can make the significant impact on the business. The paper also focuses on the challenges of blockchain which are required to address before implementation. Therefore, this paper provides an insight on the blockchain technology with the fear and smile of beginning of new era of transparency.

Keywords: Blockchain, Digital Ledger, Hashing Algorithm, Smart Contracts

1. Introduction

Now a days, the world is going through the new revolution which is known as digital revolution and it starts with the use of internet. With the usage of the internet, a new era of decentralization, no central authority, has been started, which will be supported by cryptography. Especially in the area of cryptography or digital cash, a lot of advances have been done by applying the scientific research. Earlier, the digital cash had been conceptualized with the implementation of central server which can prevent the double spending, privacy and having controlling power[1-3]. By implementing the advances of cryptography and decentralized network of computers, a new profound technology, which is known as Blockchain, has been introduced. This emerging technology has the potential to change the life of society with new rules of spending and it will be the complete paradigm shift. The decentralized system, blockchain, started a new era of global payments, corporate governance, democratic participation and functions of capital markets. The blockchain, a novel technique, can ensure the security with privacy and consensus of all the players. In the present days, the block chain has to be understood by its definition, technique and usage along with the limitations.

The blockchain can be defined as a database which is distributed, shared, encrypted and it assists to develop as an irreversible and incorruptible public repository of information[4-7]. This technology permits, for the first time, unrelated people to reach consensus on the occurrence of a particular transaction or event without the need for a controlling authority. In this technology, the security is ensured if no adversary wields a large fraction of the computational (or other forms of) resource.

The proposed technology, Blockchain technology, has the potential to reduce the role of middleman who is one of the most important economic and regulatory actors in our society. It allows the people to transfer an exclusive piece of digital property or data to others, in a safe, secure, and incontrovertible manner. Blockchain technology can create digital currencies that are not backed by any governmental body in case of demonetization. It can develop digital contracts or smart contracts, whose execution does not require any human intervention. It provides a marketplaces in decentralized manner which can be operated free from the reach of regulation[8]. It is also assisted by the decentralized platforms for communications and to monitor or spy those platforms will become more difficult in future days. It also generates the assets which are Internet-enabled assets that can be controlled just like digital property. Blockchain is a world-shattering technology, and this technology will shift the balance of power from centralized authorities in various fields like business, finance, supply chain, voting, and intellectual property and

*Author for correspondence

in politics also[9]. Therefore, it can be said that blockchain is a beginning of new era of digital property, smart contracts, decentralized governance and global capital market.

In the present paper, we have tried to understand and describe the blockchain technology. We have reviewed the literature for its definitions. We have also described the various types of the blockchain. There are three types of blockchain are in the fashion: Public, Private and Hybrid. We will elaborate all the types of blockchain. The paper also focuses on the various essential features of blockchain implementation like permissioned network, assets, transactions and consensus, a very important and unique feature. We have also done the work on its core technology, which make it safer and securer than other emerging technologies. To make it safer, the hashing algorithms have been deployed which is very difficult to wiretap. We also throw the light on the various applications of blockchain technology. Every technology has come with some limitations, therefore, we also focus on its limitations as it can eliminate many of our fundamental freedoms. Therefore, it can be said that the presented paper provides a complete overview about blockchain, which can be helpful for the future transaction in the internet based globe.

The remainder of the paper is as follows: Section 2 will describe the definitions, types and technology of blockchain while section 3 will focus on business applications of blockchain. The challenges of the evolving technology will be discussed in section 4. The paper will be concluded in section 5 with the recommendation for future work.

2. Blockchain Technology

Blockchain is the primary technology behind bitcoin and the core part of this technology is the distributed data store. All the participants in blockchain have their own data stores. The data stores store all of the transactions which has ever happened in the network. Therefore, the concept of blockchain is a distributed public ledger which is having the records of all transactions that have been performed in blockchain network and it has been shared among all the participant nodes. Each transaction in the public ledger is verified by consensus i.e. majority of the participants are agreed about the transactions. The main security feature of blockchain is that if any transaction has been entered in the public ledger, it can never be erased. Thus, the blockchain contains a certain and verifiable record of every single transaction ever made in the network. Therefore, it can be said that this technology provides a transparent network which was developed by open source, collaborative approach, and a good degree of decentralized contributed work. Firstly, we will review the various definitions of blockchain. To understand the blockchain and its information, a blockchain with two blocks is shown in Fig 1.

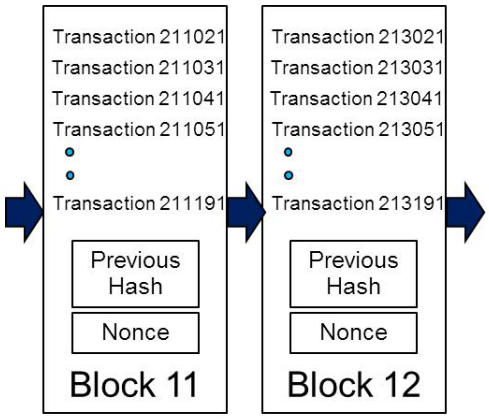

Figure 1. Schematic Diagram of Blocks.

3. Definitions

We have previously explained the blockchain in general manner and its core concepts. In the literature, we found few definitions for blockchain. According to different practitioners, the definition of blockchain is "a magic computer that anyone can upload programs to and leave the programs to self-execute, where the current and all previous states of every program are always publicly visible, and which carries a very strong crypto-economically secured guarantee that programs running on the chain will continue to execute in exactly the way that the blockchain protocol specifies."[11] This definition is given in artistic manner (magic computer) and it losses the scientific precision due to the lacking of the words like ledger, money or transactions etc. At the conceptual level, the blockchain is more informational and procedural and it cannot be said that it is limited to only financial services.

Another definition with the focus on financial services has been given[12], "If we modify our database schema so that each row can represent multiple assets, rather than the blockchain's native currency, then we can rid ourselves of that currency entirely. This leaves us with a blockchain as a way to achieve consensus and security in a peer-to-peer financial application for any class of asset." As cryptography is the essential part of the blockchain, the crypto experts said that the coin should be an integral part of the network to maintain the security.

There is myth among the practitioners that the concept of blockchain is interesting but the currency or the store of value is not very interesting. It is not possible that we cannot consider both the things separately. There should be a primary value of the token or coin (bitcoin) that's used to move value, and there is a requirement of an incentive system to create the token or coin and the created token or coin will be used for the transactions of digital property[13].

4. Types of Blockchain

After the understanding of blockchain in the definitions, we will discuss the various types of blockchains. There are three types of blockchains: Private, Public and Hybrid blockchains. We will discuss the nature of each type of blockchain which will help us to understand the core concept of each blockchain.

In the Public blockchain, the digital ledger is completely decentralized and it can be accessible to any Internet user. The public blockchain is having the nature of free and unconditional participation of everyone in the process. The participants will decide about the current state of blockchain and what kind of blocks will be added to the chain. For validation of transactions, the public blockchain relies on consensus mechanism of proof-of-work. Especially in the case of Bitcoin, the longest chain – the chain with the most proof-of-work – is considered to be the valid ledger.

As intended in the name, the entries in a fully private blockchain are monitored by a central authority of decision-making for writing permission. For read-permissions, it may be restricted to the participants or open to all the users. In a private blockchain, an organization can listed down the users based on the process of Know-Your-Business (KYB) and Know-Your-Customer (KYC). The difference between public and private blockchains is the extent to which they are decentralized, or ensure anonymity.

Between the two extremes, there exists a continuum of "partially decentralized" blockchains, rather than a strict public/private dichotomy. Partially decentralized, also called "consortium blockchains", constitute a hybrid between the low-trust (i.e. public blockchains) and the single highly-trusted entity model (i.e. private blockchains)[14]

5. Features

A distributed database of records of all the transactions, which are happened and shared among all the participant nodes, called the blockchain. The transactions are happened due to the available digital assets like one will send the digital assets to someone. The information of transactions will be shared as per the nature of network. For each transaction, the consensus is important i.e. if majority of all the parties verified the transaction, it will be validated. We can understand the logic by an analogy like stealing a chocolate from fridge in kitchen is easier than stealing the chocolate from fridge which is kept in the observation of thousand people. Therefore, there are some essential features of blockchain which we will discuss in detail (figure 2):

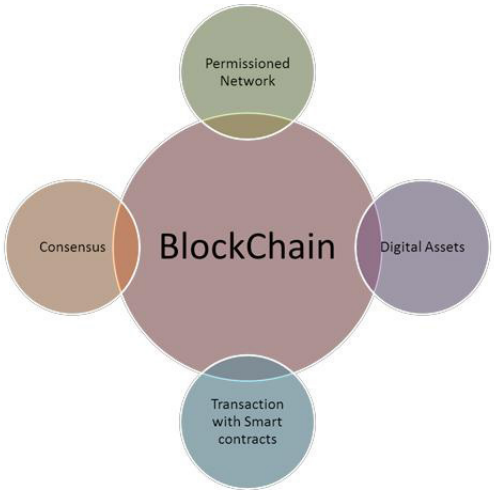

Figure 2. Features of Blockchain.

1) Permissioned Network: Firstly, a network is created and genuine members or participants are invited in the network. The write or read permission will be provided according to the role of participants. In this network, all the transactions are shared with each participants in the network, but permissions can control who has the right to view or modify those transactions.

2) Assets: Assets can be created on a network using smart contracts and can be tangible or intangible such as intellectual property, art, financial assets, car leases or shipping containers full of goods.

3) Transactions: A transaction is created in blockchain, when any digital asset is transferred. A block has been formed with multiple transactions and it is secured by hash. The transaction entry is made ineradicable by hashing the transactions with the previous blocks, thus chaining them together.

4) Consensus: We need a way to tell if the transactions are authentic or not and if the members agree to those transactions. Consensus is the way to achieve that, where members vote on the validity of a transaction.

These key features now enable us to settle a transaction in seconds compared to days. As we have discussed the essential features of the blockchain. We will discuss the technology which make the blockchain safer and secured.

6. Block Hash Algorithm

There are many techniques in cryptography for e.g. public key cryptography where each coin is associated with it current owner's Elliptic Curve Digital Signature Algorithm key.

When a party send a bitcoin to another party, it is basically creating a transaction and new owner's public key is attached to the amount of coins being transferred and sign it with the private key and this transaction shows up on the bitcoin network which inform everyone about the new owner. There are signature on every message which is an evidence of its authenticity and the history will be kept by everyone for future references[2].

A transaction is basically a sequence of records called Blocks and the record of each and every transaction is like a chain which makes it a block chain. Everyone in the network is have a copy of Block Chain which can be updated by passing the new blocks on it. Each Block in the chain occurs after the previous one which proves that the previous one was authenticated.

To make sure the security of bitcoins, there is function called HashCash is used. Hashcash is the first secure efficiently verifiable cost-function or proof-of-work function. The beauty of hashcash is that it is non-interactive and has no secret keys that have to be managed by a central server or relying party; hashcash is as a result fully distributed and infinitely scalable. (Hashcash uses symmetric key cryptography, namely a one-way hashcash function - typically either SHA1 or SHA-256)[3].

Hash function is flexible enough to take any kind and size of a data as an input, transforms it in an effectively-impossible to reverse or to predict way, into a relatively compact string. Making a little change to an input data changes its hash by which no one can create a different block of data that gives exactly the same hash. The blocks, which do not have a serial number and can be identified by their hash, serves the dual purpose of identification as well as integrity verification. An identification string that also provides its own integrity is called a self-certifying identifier. The hashcash cost-function iterates by altering data in the block by a nonce value, until the data in the block hashes to produce an integer below the threshold - which takes a lot of processing power. This low hash value for the block serves as an easily-verifiable proof of work - every node on the network can instantly verify that the block meets the required criteria (Fig 3).

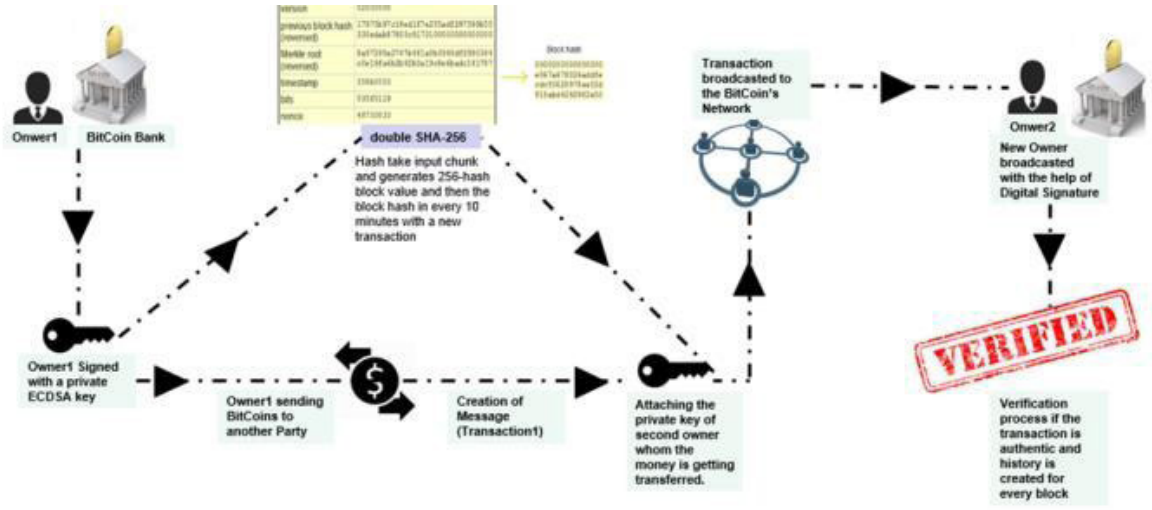

Figure 3. End to End process of Bitcoin.

After discussing the blockchain technology with its features and core technology of hashing, we will explore the different areas of application.

7. Business Applications of Blockchain

In this section, we will review the opportunities of blockchain implementation in various business applications. Still the blockchain is not widely used in the business applications but due to its inherent transparency and consensus based validation, it can be applied in various fields like finance, supply chain, healthcare, government services, social services, money laundering etc. The applications are shown in figure 4.

The potential application areas of the blockchain are very widespread. We have classified the areas of application on the basis of the services provided by blockchain. According to figure 4, we can understand that one of the most important service is the transactions in digital currencies. With the service of digital currencies, the blockchain can change the future of e-commerce business. In e-commerce business, one participant can sell the assets and other party will pay in digital currency and it will be verified by all the participants[8]. This is another step towards cashless transactions. It is also useful for global payments due to the different currencies in different countries and buyer and seller can be from different countries and they can pay using digital currency. For peer-to-peer lending, it is the best way to lend the money and track the transactions.

The applications of digitized ledger is very high in all the areas and industries. It is highly applicable in healthcare industry for record keeping of health reports and issues. It is equally applicable for ownership of property and keep all the records for personal use and for government processes. It is like the digital wallet of all the ownership as well as personal identification documents. The blockchain is highly recommended for supply chain as there are so many materials, peoples and places are involved. To manage the supply chain efficiently, each and every transaction should be recorded from each people and location. In each process of supply chain, a lot of peoples are involved, therefore, consensus should be given by all the participants to validate the transaction of goods or payments. The blockchain can be applicable in government services like aadhar card, passport service etc[6].

It provides a secured network which is essentially required in the business of equity and derivatives as there are lot of opportunities of fraud or double spending. The secured network with hashing algorithm can prevent any alteration in the transaction. Therefore, it is very safe and secured network and highly applicable in financial transactions. With the feature of smart contracts, blockchain can be applicable in digital rights, betting and to decide the terms and conditions for loaning between two participant parties.

From the above, it can be said that blockchain technology is applicable in various industries and different business lines. It can also be said that blockchain technology is equally applicable in financial as well as non-financial industries. It can be applied in other social work like donations, marriage etc. With the widespread applications of the blockchain, we have to have an eye on the limitations of the blockchain.

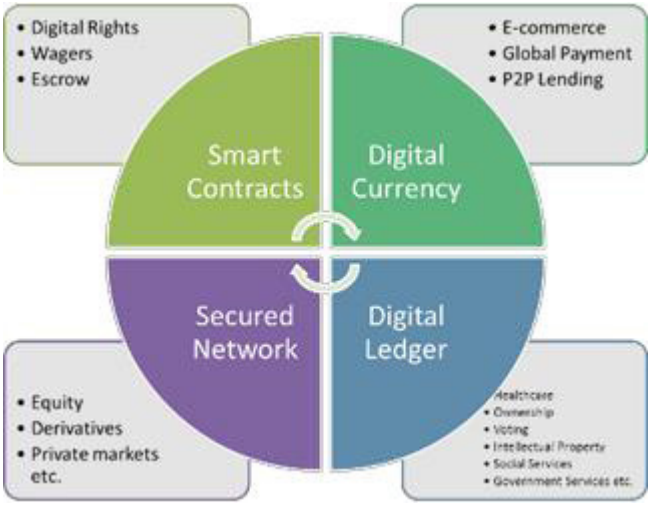

Figure 4. Applications of Blockchain.

8. Challenges

There are a lot of challenges imposed as blockchain is an evolving technology and still in developing stage. Those challenges are related to technical issues, business models, regulatory of government and adoption of the new technology. We will discuss the various challenges of blockchain technology in the light of various facts.

In the blockchain technology, there are several technological issues related to implementation and development or coding. There is another challenge related to the scaling up of the block generation speed from 6 per hour to 12 per hour. Now a days, the block has the maximum limit of 7 transactions per second but in financial services, it is sometimes 2000 transactions per second. So, the people are facing the challenge of scaling up. There is a security feature in blockchain that no one can erase any transaction but at the same time it becomes a limitation to modify the previous transactions. Some other technical issues have to do with the infrastructure. One issue is the explosion of blockchains, as there are so many different blockchains in existence. Another issue is that when chains are split for administrative or versioning purposes, there is no easy way to merge or cross-transact on forked chains[3,6]. The other issues are related to the infrastructure like data storage, cloud infrastructure, network administration, name and space management etc. Along with the technical challenges, blockchain is also facing some business challenges.

In business modelling, the reconfiguration of the entire business models with smart contracts and new rules is very difficult to implement. The main challenge is to make it completely decentralized without any transaction fee. The adoption of the Bitcoin for the transactions is another challenge for the business. As it is decentralized, there is another threat related to illegal activities like money laundering, smuggling, drug dealing etc. Another challenge is related to the implementation of government regulations like taxation, calculations for GDP etc. For the adoption it widely, peoples are having the threat like privacy. Those are the issues or perception which will be the biggest obstacles for widespread implementation.

However, with all of those probable challenges with blockchain, it can be said that blockchain is good for various business especially in education and healthcare and its impact will be significant. There are some solutions provided to overcome the technical challenges and the blockchain industry is working on it but on the other hand, we have to spread the awareness about its impact and advantages.

9. Conclusion

In this paper, we have discussed the concepts of blockchain technology with definitions as well as some of the significant features of blockchain. We have shown that this technology is emerging and make a new revolution in the financial services along with other applications in other business. We have also discussed the challenges of the blockchain. It works in un-trust environment only with consensus and people required the trust business but in the contrary the trust is not always a good thing because it increases the bond among gang members. Therefore, the blockchain technology can work excellently in major business where number of transactions are very high like financial services, supply chain, government services etc. The blockchain will increase the effectiveness and efficiency of the system by the inherency of transparency. We believe that the blockchain is still in infancy stage and in the near future, it will be more matured and applicable in other areas like sports, games, tourism etc.

10. References

1. Bohme R, Christin N, Edelman B, Moore T. Bitcoin: Economics, Technology, and Governance. Journal of Economic Perspectives. 2015; 29(2):213–38. https://doi.org/10.1257/jep.29.2.213
2. Swanson T. Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems. 2015.
3. Sahni N. A Review on Cryptographic Hashing Algorithms for Message Authentication. International Journal of Computer Applications. 2015; 120(16). https://doi.org/10.5120/21313-4290
4. Lin K, Yang H-F, Hsiao J-H, Chen C-S. Deep learning of binary hash codes for fast image retrieval. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops. 2015. p. 27–35. https://doi.org/10.1109/cvprw.2015.7301269
5. Mattila J, Seppala T, Naucler C, Stahl R, Tikkanen M, Badenlid A, Seppala J. Industrial Blockchain Platforms: An Exercise in Use Case Development in the Energy Industry. The Research Institute of the Finnish Economy. 2016; 43.
6. Kishigami J, Fujimura S, Watanabe H, Nakadaira A, Akutsu A. The Blockchain-Based Digital Content Distribution System. 2015 IEEE Fifth International Conference on Big Data and Cloud Computing (BDCloud), IEEE. 2015. p. 187–90. https://doi.org/10.1109/BDCloud.2015.60
7. Watanabe H, Fujimura S, Nakadaira A, Miyazaki Y, Akutsu A, Kishigami JJ. Blockchain contract: A complete consensus using blockchain. In 2015 IEEE 4th Global Conference on Consumer Electronics (GCCE), IEEE. 2015. p. 577–8. https://doi.org/10.1109/gcce.2015.7398721
8. Swan M. Blockchain: Blueprint for a new economy. O'Reilly Media, Inc. 2015.
9. Fay T, Paniscotti D. Systems and methods of blockchain transaction recordation. U.S. Patent Application 15/086,801, filed Mar 31, 2016.
10. Avital M, Beck R, King J, Rossi M, Teigland R. Jumping on the Blockchain Bandwagon: Lessons of the Past and Outlook to the Future. 2016.
11. Devine P. Blockchain learning: can crypto-currency methods be appropriated to enhance online learning? 2015.

12. Pilkington M. Blockchain technology: principles and applications. Research Handbook on Digital Transformations, edited by F. Xavier Olleros and Majlinda Zhegu. Edward Elgar. 2016.
13. Fujimura S, Watanabe H, Nakadaira A, Yamada T, Akutsu A, Kishigami JJ. BRIGHT: A concept for a decentralized rights management system based on blockchain. 2015 IEEE 5th International Conference on Consumer Electronics-Berlin (ICCE-Berlin), IEEE. 2015. p. 345–6. https://doi.org/10.1109/icce-berlin.2015.7391275
14. Atzori M. Blockchain-Based Architectures for the Internet of Things: A Survey. Browser Download This Paper. 2016.

Citation:

K. Siba, Tarun and Anuj Prakash
"Block-Chain: An Evolving Technology",
Global Journal of Enterprise Information System. Volume-8, Issue-4, October-December, 2016.
(http://informaticsjournals.com/index.php/gjeis)

Conflict of Interest:

Author of a Paper had no conflict neither financially nor academically.