Journal of Contemporary Issues in Business and Government Vol. 27, No. 02, 2021
https://cibg.org.au/

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2021.27.02.657

A Survey on Block chain Technology beyond Bitcoin

Soumen Paul[1*], Ramkrishna Ghosh[2*]

[1,2]Department of Information Technology

Haldia Institute of Technology, Haldia,West Bengal, India

[1]s.paul.it@gmail.com, [2]ramkr.ghosh@gmail.com

Abstract: A Blockchain (BC) is essentially a distributed database of records or public ledger of all transactions or digital events that have been executed and shared among participating parties. Each transaction in the public ledger is verified by consensus of a majority of the participants in the system. And, once entered, information can never be erased. The BC contains a certain and verifiable record of every single transaction ever made. Bitcoin, the decentralized peer to peer digital currency, is the most popular example that uses BC technology. The digital currency bitcoin itself is highly controversial but the underlying BC technology has worked flawlessly and found wide range of applications in both financial and nonfinancial world. The main hypothesis is that the BC establishes a system of creating a distributed consensus in the digital online world. This allows participating entities to know for certain that a digital event happened by creating an irrefutable record in a public ledger. It opens the door for developing a democratic open and scalable digital economy from a centralized one. There are tremendous opportunities in this disruptive technology and revolution in this space has just begun. This white paper describes BC technology and some compelling specific applications in both financial and nonfinancial sector. We then look at the challenges ahead and business opportunities in this fundamental technology that is all set to revolutionize our digital world.

Keyword: Blockchain, Bitcoin, Public Ledger, Distributed Consensus.

I. Introduction

Nowadays crypto currency has become a buzzword in both industry and academia. As one of the most successful cryptocurrency, Bitcoin has enjoyed a huge success with its capital market reaching 10 billion dollars in 2016 [1]. 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 [2]. A Blockchain is fundamentally a disseminated database of records or public ledger of all communications or digital proceedings that have been executed and shared among participating parties. Each transaction in the public ledger is confirmed by consensus of a majority of the participants in the system. And, once entered, information can never be erased. The block chain contains a certain and confirmable record of every single transaction still made. To use a basic analogy, it is easy to steal a cookie from a cookie jar, kept in a secluded place than stealing the cookie from a cookie jar kept in a market place, being observed by thousands of people. Bitcoin is the most popular example that is intrinsically tied to blockchain technology. It is also the most controversial one since it assists to facilitate a multibillion-dollar global market of anonymous transactions without any

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2021.27.02.657

governmental control. Hence it has to deal with a number of regulatory issues involving national governments and financial institutions.

However, Blockchain technology itself is non-controversial and has worked faultlessly over the years and is being successfully functional to both financial and non-financial world applications. Last year, Marc Andreessen, the doyen of Silicon Valley's capitalists, listed the block chain distributed consensus model as the most important invention since the Internet itself. Johann Palychata from BNP Paribas wrote in the Quintessence magazine that bitcoin's blockchain, the software that permits the digital currency to role should be considered as an invention like the steam or burning engine that has the potential to change the world of finance and beyond

According to Author Miraz et. al. [3] the goal of their research paper is to summarize the literature on achievement of the Blockchain and similar digital ledger methods in a range of other domains beyond its purpose to crypto-currency and to depict appropriate conclusions. Blockchain being comparatively a new technology, a representative example of research is accessible, spanning over the last ten years, starting from the early work in this field. Different types of practice of Blockchain and other digital ledger techniques, their challenges, applications, security and privacy issues were examined. Identifying the most auspicious direction for future use of Blockchain beyond crypto-currency is the main focal point of the assessment study. This is where the blockchain technology comes useful. It has the potential to modernize the digital world by facilitating a scattered consensus where each and every online transaction, past and present, concerning digital assets can be confirmed at any time in the future. It does this without co-operating the privacy of the digital assets and parties involved. The distributed consensus and anonymity are two significant characteristics of blockchain technology. The advantages of Blockchain technology outweigh the regulatory issues and technical challenges. One key emerging use case of blockchain technology involves "smart contracts". Smart contracts are basically computer programs that can automatically execute the terms of a contract. When a pre-configured condition in a smart contract among participating entities is met then the parties involved in a contractual agreement can be automatically made payments as per the contract in a transparent manner.

Smart Property is another correlated thought which is regarding controlling the ownership of a property or asset via blockchain using Smart Contracts. The property can be physical such as car, house, Smart phone etc. or it can be non-physical such as shares of a company. It should be noted here that even Bitcoin is not actually a currency--Bitcoin is all about controlling the ownership of money. According to author Miraz [4] by applying Blockchain or similar crypto-currency practices, the users neither require to trust each other nor do they want an intermediator; rather the trust is manifested within the decentralized network system itself. Blockchain thus comes out to be the supreme "Trust Machine" pattern. Zheng et. al. [5] in their paper, they provide an overview of blockchain architechture firstly and compare some typical consensus algorithms used in different blockchains. Moreover, technical challenges and recent advances are briefly listed. We also lay out possible future trends for blockchain. Since Blockchain allows payment to be finished without any bank or any intermediary, blockchain can be used in various financial services such as digital assets, remittance and online payment [6], [7]. Additionally, it can also be applied into other fields including smart contracts [8], public services [9] Internet of including Bitcoin. Authors in [19],[20],[21],[22] have shown interest in Blockchain technology.

The rest of this paper is organized as follows. Section II shows Short history of bitcoin, Section III summarizes Different approaches to overcome the limitations of Bitcoin blockchain, Section IV discusses Working of Blockchain Technology . Section V discusses challenges and recent advances and section VI concludes the paper.

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2021.27.02.657

II. Short History of Bitcoin

In year 2008, an individual or group writing under the name of Satoshi Nakamoto published a paper entitled "Bitcoin: A Peer-To-Peer Electronic Cash System". This paper described a peer-to-peer version of the electronic cash that would permit online payments to be sent openly from one party to another without going through a financial institution. Now word crypto currencies is the marker that is used to explain all networks and mediums of switch that uses cryptography to secure transactions-as in opposition to those systems where the transactions are channeled through a central trusted thing.

– 2008

- **August 18** Domain name "bitcoin.org" registered
- **October 31** Bitcoin design paper published
- **November 09** Bitcoin project registered at SourceForge.net

– 2009

- **January 3** Genesis block established at 18:15:05 GMT
- **January 9** Bitcoin v0.1 released and announced on the cryptography mailing list
- **January 12** First Bitcoin transaction, in block 170 from Satoshi to Hal Finney

The recognition of the Bitcoin has never ceased to increase since then. The underlying BlockChain technology is now finding innovative range of applications beyond finance.

III. Different approaches to overcome the limitations of Bitcoin blockchain

Alternative Blockchains is a system of using the blockchain algorithm to achieve distributed consensus on a particular digital asset. They may share miners with a parent network such as Bitcoin's--this is called merged mining. They have been suggested to implement applications such as DNS, SSL certification authority, file storage and voting.

Colored Coins is an open source protocol that describes class of methods for developers to create digital assets on top of Bitcoin blockchain by using its functionalities beyond digital currency.

Sidechains are substitute blockchains which are backed by Bitcoins via Bitcoin contract--just as dollars and pounds used to be backed by Gold. One can perhaps have a thousands of sidechains pegged" to Bitcoin, all with different uniqueness and purposes "all of them taking benefit The Bitcoin blockchain can in turn iterate to maintain additional features for the experimental side chains--once they have been attempted and tested.

IV. Working of Blockchain Technology

We clarify the perception of the blockchain by explaining how Bitcoin works since it is intrinsically linked to the Bitcoin shown in Fig 1. However, the blockchain technology is applicable to any digital asset transaction exchanged online. Internet commerce is exclusively tied to the financial institutions serving as the trusted third party who process and mediate any electronic transaction. The role of trusted third party is to authenticate, safeguard and protect transactions. A certain percentage of fraud is unavoidable in online transactions and that needs mediation by financial transactions. This results in

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2021.27.02.657

high transaction costs. Each transaction is protected through a digital signature. Each transaction is sent to the "public key" of the receiver digitally signed using the "private key" of the sender. In order to spend money, owner of the cryptocurrency needs to prove the ownership of the "private key". The entity receiving the digital currency verifies the digital signature – thus ownership of corresponding "private key"--on the transaction using the "public key" of the sender.

Verifying node needs to ensure two things before recording any transaction:

1. Spender owns the cryptocurrency—digital signature verification on the transaction.
2. Spender has adequate cryptocurrency in his/her account: checking every transaction against spender's account ("public key") in the ledger to make sure that he/she has ample balance in his/her account.

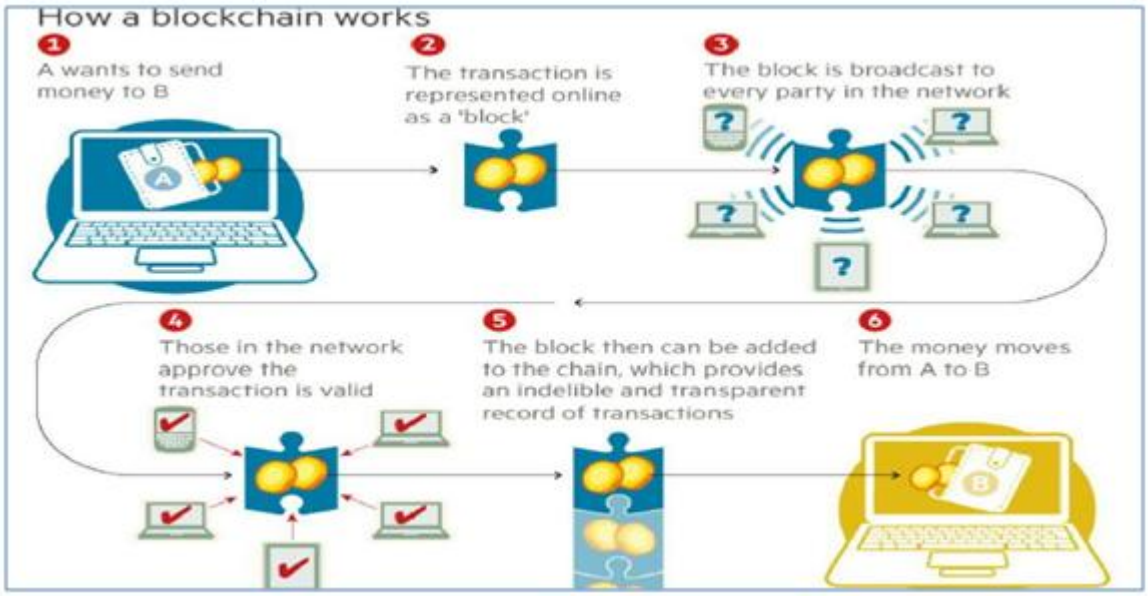

Fig 1. Financial Transactions using the Blockchain technology

However, there is question of maintaining the order of these transactions that are broadcast to every other node in the Bitcoin peer-to-peer network shown in Fig 2. The transactions do not come in order in which they are generated and hence there is need for a system to make sure that double-spending of the cryptocurrency does not occur. Considering that the transactions are passed node by node through the Bitcoin network, there is no guarantee that orders in which they are received at a node are the same order in which these transactions were generated.

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2021.27.02.657

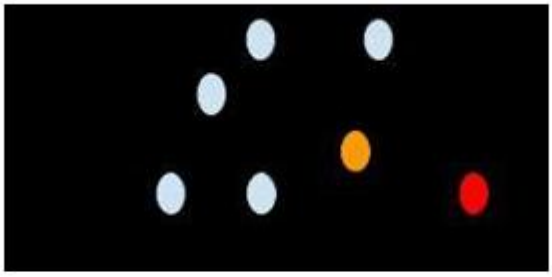

Fig 2. Double spending due to propagation delays in peer-to-peer network

This means that there is requirement to extend a method so that the entire Bitcoin network can agree regarding the order of transactions, which is an overwhelming task in a distributed system. There still remains one problem. Any node in the network can collect unconfirmed transactions and create a block and then broadcasts it to rest of the network as a suggestion as to which block should be the next one in the blockchain. How does the network decide which block should be next in the blockchain? There can be multiple blocks created by different nodes at the same time. One can't rely on the order since blocks can arrive at different orders at different points in the network. The Bitcoin solved this problem by a mechanism that is now commonly known as Blockchain technology. The Bitcoin system orders transactions by placing them in groups called blocks and then linking these blocks through what is called Blockchain. The transactions in one block are measured to have happened at the same time. These blocks are linked to each-other (like a chain) in a proper linear, chronological order with every block containing the hash of the previous block.

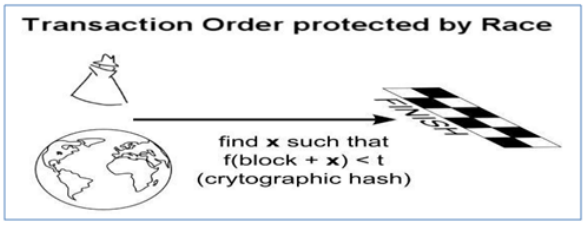

Fig 3: Mathematical race to protect transactions-I

This is also known as "proof of work"—node generating a block needs to prove that it has put enough computing resources to solve a mathematical puzzle shown in Fig. 3. For instance, a node can be required to find a "nonce" which when hashed with transactions and hash of previous block produces a hash with certain number of leading zeros. The average effort required is exponential in the number of zero bits required but verification process is very simple and can be done by executing a single hash.

This mathematical puzzle is not insignificant to solve and the complexity of the problem can be adjusted so that on average it takes ten minutes for a node in the Bitcoin network to make an accurate guess and generate a block. There is very small probability that more than one block will be generated in the system at a given time. First node, to solve the problem, broadcasts the block to rest of the network. Occasionally, however, more than one block will be solved at the same time, leading to several possible branches. However, the math of solving is very complicated and hence the blockchain rapidly stabilizes, meaning that every node is in conformity about the ordering of blocks a few back from the end of the chain. The

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2021.27.02.657

nodes donating their computing resources to solve the puzzle and generate block are called "miner" nodes" and are financially awarded for their efforts.

V. Challenges & Recent Advances

A. Scalability

Despite the large possible of blockchain, it faces abundant challenges, which limit the wide usage of blockchain. We itemize some major challenges and recent advances as follows. A. Scalability With the amount of transactions increasing day by day, the blockchain becomes bulky. Each node has to store all transactions to validate them on the blockchain because they have to check if the source of the current transaction is unspent or not. Besides, due to the original restriction of block size and the time interval used to generate a new block, the Bitcoin blockchain can only process nearly 7 transactions per second, which cannot fulfill the requirement of processing millions of transactions in real-time fashion. Meanwhile, as the capacity of blocks is very small, many small transactions might be delayed since miners prefer those transactions with high transaction fee. There are a number of efforts proposed to address the scalability problem of blockchain, which could be categorized into two types: 1) Storage optimization of blockchain 2) Redesigning blockchain.

B. Privacy Leakage

Blockchain can preserve a certain amount of privacy through the public key and private key. Users transact with their private key and public key without any real identity exposure.However, it is shown in [10], [11] that blockchain cannot guarantee the transactional privacy since the values of all transactions and balances for each public key are publicly visible. Besides, the recent study [12] has shown that a user's Bitcoin transactions can be linked to reveal user's information.

Moreover, Biryukov et al. [13] presented an method to link user pseudonyms to IP addresses even when users are behind Network Address Translation (NAT) or firewalls. In [13], each client can be uniquely identified by a set of nodes it connects to. However, this set can be learned and used to find the origin of a transaction. Multiple methods have been proposed to progress anonymity of blockchain, which could be roughly categorized into two types:

1. Mixing [14] 2. Anonymous.

C. Selfish Mining

Blocks without broadcasting and the private branch would be exposed to the public only if some requirements are satisfied. As the private branch is ineffective branch while selfish miners are mining their private chain without competitors. So selfish miners be likely to get more revenue.

Based on selfish mining, many other attacks have been planned to show that blockchain is not so protected. In stubborn mining [16], miners could strengthen its gain by non-trivially composing mining attacks with network-level eclipse attacks.

D. Blockchain applications

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2021.27.02.657

Currently most blockchains are used in the financial domain, more and more applications for different fields are appearing. Traditional industries could take blockchain into consideration and apply blockchain into their fields to enhance their systems. For example, user reputations could be stored on blockchain. At the same time, the up-and-coming industry could make use of blockchain to improve performance. For example, Arcade City [17], a ridesharing startup offers an open marketplace where riders connect directly with drivers by leveraging blockchain technology.

A smart contract is a computerized transaction protocol that executes the terms of a contract [18]. It has been proposed for long time and now this concept can be implemented with blockchain. In blockchain, smart contract is a code fragment that could be executed by miners automatically. Smart contract has transformative potential in various fields like financial services and IoT.

VI. Conclusion

To conclude, Blockchain is the technology backbone of Bitcoin. The distributed ledger functionality coupled with security of BlockChain, makes it very attractive technology to solve the current Financial as well as non-financial business problems. There is enormous interest in BlockChain based business applications and hence numerous Start-ups working on them .The adoption definitely faces strong headwind. The large Financial institutions like Visa, Mastercard, Banks, NASDAQ, etc., are investing in exploring application of current business models on BlockChain. In fact, some of them are searching for the new business models in the world of BlockChain. To conclude, we envision BlockChain to go through slow adoption due to the risks associated. Most of the Startups will fail with few winners. We should be seeing significant adoption in a decade or two.

References

[1] “State of blockchain q1 2016: Blockchain funding overtakes bitcoin,” 2016. [Online]. http://www.coindesk.com/ state-of-blockchain-q1-2016

[2] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[3] M. H. Miraz, M. Ali, Applications of Blockchain Technology beyond Cryptocurrency, Annals of Emerging Technologies in Computing (AETiC) Vol. 2(1) 2018,1-6.

[4] M. 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

[5]. Z.Zheng, S. Xie, H. Dai, X. Chen, H. Wang, An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends, 2017 IEEE 6th International Congress on Big Data, 557-564.

[6] G. Foroglou and A.-L. Tsilidou, “Further applications of the blockchain,” 2015.

[7] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, “Hawk: The blockchain model of cryptography and privacy-preserving smart contracts,” in Proceedings of IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 2016,839–858.

[9] Y. Zhang and J. Wen, “An iot electric business model based on the protocol of bitcoin,” in Proceedings of 18th International Conference on Intelligence in Next Generation Networks (ICIN), Paris, France, 2015, 184–191.

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2021.27.02.657

[10] S. Meiklejohn, M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G. M. Voelker, and S. Savage, "A fistful of bitcoins: Characterizing payments among men with no names," in Proceedings of the 2013 Conference on Internet Measurement Conference (IMC'13), New York, NY, USA, 2013.

[11] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in Proceedings of IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 2016, 839–858.

[12] J. Barcelo, "User privacy in the public bitcoin blockchain," 2014.

[13] A. Biryukov, D. Khovratovich, and I. Pustogarov, "Deanonymisation of clients in bitcoin p2p network," in Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, New York, NY, USA, 2014, pp. 15–29.

[14] M. M¨oser, "Anonymity of bitcoin transactions: An analysis of mixing services," in Proceedings of M¨unster Bitcoin Conference, M¨unster, Germany, 2013, pp. 17–18.

[15] NRI, "Survey on blockchain technologies and related services," Tech. Rep., 2015. [Online]. Available: http://www.meti.go.jp/english/press/ 2016/pdf/0531 01f.pdf

[16] K. Nayak, S. Kumar, A. Miller, and E. Shi, "Stubborn mining: Generalizing selfish mining and combining with an eclipse attack," in Proceedings of 2016 IEEE European Symposium on Security and Privacy (EuroS&P), Saarbrucken, Germany, 2016, pp. 305–320.

[17] S. Solat and M. Potop-Butucaru, "ZeroBlock: Timestamp-Free Prevention of Block-Withholding Attack in Bitcoin," Sorbonne Universites, UPMC University of Paris 6, Technical Report, May 2016. [Online]. Available: https://hal.archives-ouvertes.fr/hal-01310088

[18] N. Szabo, "The idea of smart contracts," 1997.

[19] B. W. Akins, J. L. Chapman, and J. M. Gordon, "A whole new world: Income tax considerations of the bitcoin economy," 2013. [Online]. Available: https://ssrn.com/abstract=2394738.

[20] Y. Zhang and J. Wen, "An iot electric business model based on the protocol of bitcoin," in Proceedings of 18th International Conference on Intelligence in Next Generation Networks (ICIN), Paris, France, 2015, 184–191.

[21] C. Noyes, "Bitav: Fast anti-malware by distributed blockchain consensus and feedforward scanning," arXiv preprint arXiv:1601.01405, 2016.

[22] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," in Proceedings of International Conference on Financial Cryptography and Data Security, Berlin, Heidelberg, 2014, 436– 454.