J. Sustain. Wireless Syst.
Vol.02/ No. 1
Pages: 13-22
http://irojournals.com/irosws/
DOI: https://doi.org/10.36548/jsws.2020.1.002

Technical Scrutiny of Block chain Technology Protocols and its Applications

Madhura.S
ECE Deaprtment, RV Institute of Technology and Management
Bangalore,India
madhuras.rvitm@rvei.edu.in

Shubham Luharuka
CSE Deaprtment, RV Institute of Technology and Management
Bangalore,India
luharukas@yahoo.com

Gaurav Anil Kulkarni
CSE Deaprtment, RV Institute of Technology and Management
Bangalore,India
kulkarnigaurav38@gamil.com

Pallothu Devi Sri
CSE Deaprtment, RV Institute of Technology and Management
Bangalore,India
pallothudevisri@gmail.com

Ria Somani
CSE Deaprtment, RV Institute of Technology and Management
Bangalore,India
ria.somani316@gmail.com

Abstract—Block chain technology is one which is evolving over time and is still brand new to the mindset of various people. The question of how to use it even if one has the want to use it arises thereby questioning its need in necessary functioning. This technology may be hand in hand if required for the following features:-Various distributed participants; lack of trust in mediating parties; if maximum work is done through transactions. A need to reduce manual labor and be comfortable with digital listing of activities to avoid disputes. When one has a real time need of sharing the various activities with other clients/partners and get a valid and crisp work history. In this paper the importance of block chain and its implications are presented along with various case studies of technical glitches whether in IoT or banking sectors, this paper covers it all.

Keywords—Block Chain, IoT, machine learning, Artificial Intelligence**.**

1. Introduction

Block chains are distributed (i.e., without a central repository), tamper resistant, sharing platforms that allows multiple authoritative domains, who do not trust each other, to work together in application development process or business development process. Block chain can be thought of as a distributed database which accommodates and thus helps in cooperation between multiple authoritative domains providing strong consistency support. Basically, they enable a community of users to record transactions in a public (shared) ledger within that community. It has the distinct advantage over a central authority which can act as a single point of failure, but due to the distributed (decentralized) fashion of the Blockchain network, failures of multiple servers also doesn't hurt the smooth conduct of the system and are robust to failure [1]. Each member (node) of the distributed network maintains a local copy (personal copy) of the global data sheet which can be validated on their own. Blockchain network ensures that they keep viewing the most updated copy, time to time.

The main basis of the architectural platform of this network is that if one node wants to enter some information to the network, then this new information should get updated to each of the local copies of all the nodes in the network such that it maintains a strong consistency in the data that every node possesses. This along with cryptographic hashed system makes Blockchain very secure and almost impossible to hack.

ISSN: 2582-3167 (online)

IRO Journal on Sustainable Wireless Systems (2020)
Vol.02/ No. 1
Pages: 13-22
http://irojournals.com/irosws/
DOI: https://doi.org/10.36548/jsws.2020.1.002

1.1. IMPORTANT TERMS RELATED TO BLOCKCHAIN

A. Ledgers:

Periodic and appropriate backup of system by the owner should be trusted by the user.

- Usually all centrally owned ledger has the same geographical locations but network issues at that place would thereby result in unavailability of ledges and other services. Trust the centralized system is a must since not all transactions and workings will be transparent. The list may not be complete as well since all details cannot be displayed. Insecurities may cause hostility between user and centralized system preventing a harmony in the working.

B. Blocks:

A block is an essential part of a block chain technology system. The users send transaction information to the network which is thereby forwarded to nodes within the network. It is then added to the block chain by an established node until then the transaction is supposed to wait in a queue. A block has two parts – block header and block data. A block header has metadata (data that describes other data, serving as an informative label) inscribed in it. The block data contains the list of established and authorized transactions that have been provided to the network [2]. The efficacy and reliability of transactions is ensured by keeping a check on the informations being input and the validity of the digital assets over which a digital signature is then given. Generally, following data fields are defined by various block chains:-

a) Block Header:

- The block number or block height
- Hash value of previous block headers and its hash representation.
- Timestamp
- Block size
- Nonce value

b) Block Data: The list of valid transactions is foremost important in the data for the block to be established and other data information may be present.

C. Transcations:

Transactions represent digital communications between the various users of a block chain system. It also enables to record asset processes occurring digitally. Different transactions shall evidently comprise of various data but the general working for transaction always remains the same. Addition of more blocks even with no transactions prevents

ISSN: 2582-3167 (online)

IRO Journal on Sustainable Wireless Systems (2020)
Vol.02/ No. 1
Pages: 13-22
http://irojournals.com/irosws/
DOI: https://doi.org/10.36548/jsws.2020.1.002

'malicious threats' since it keeps the hacker from knowing the transaction inputs/outputs. The user gives input thereby supplying the details to the network which may include the sender's details, transaction details, etc.

Hence transactions can be used to share data, analyze data and get some output for the block chain. The efficacy of a transaction enables it to meet a particular set of regulations. The reliability of a transaction highlights that the user has control to its own digital input assets.

D. Chaining Blocks:

Each block header contains the hash value of the previous block as described earlier. This helps in chaining the block and easy debugging in case of any alteration since all the blocks are interlinked through secure digital hash numbers.

E. Addresses and Address Derivation:

Some networks include the functioning of address, which is formed using cryptographic hash function on the public key along with some additional data. Addresses are shorter and not a secretive attribute. Every implementation may make use of different methods but generally these addresses are converted into a QR code and made easy to use through mobile phones, tabs and other devices. One of the several methods to form an address is Create a public key, Modify using hash functions, Generation of address.

F. Private Key Storage:

It is a very important facet of block chain technology. As discussed earlier, private key is associated with every minute information from the user and enables in carrying out transactions as well. Rather than manually storing these keys, software called wallet is often used. It enables to keep up with the security attribute of the entire technology. If a private key is lost, every asset linked to it is lost since this advantage of not being able to encrypt another private key of the same relevant information serves as a drawback here. Security of these private keys is hence of immense importance.

G. Forking:

Fork is a thing which happens when a block chaintries to make a new rule in deciding whether the transaction is valid or not. Forks are of three different types:

Temporary fork:- The temporary forks occurs when miners ,who can develop coin in block chain , finds a block at a same time at two different places , which will result in two splits in block chain. Temporary forks differ from soft forks and hard forks, as soft fork and hard fork will represent a permanent changes in their rules.

ISSN: 2582-3167 (online)

IRO Journal on Sustainable Wireless Systems (2020)
Vol.02/ No. 1
Pages: 13-22
http://irojournals.com/irosws/
DOI: https://doi.org/10.36548/jsws.2020.1.002

Soft forks:-The soft forks are backward compatible with previous blocks, that means it also accepts the blocks which are following the previous versions of software

Hard forks:- Unlike soft forks, hard fork requires all nodes to upgrade to the latest version of rules of software.

2.CRYPTOGRAPHIC HASH FUNCTIONS

Hashing is a method in which a given input of any size gives an output of a fixed size. Cryptographic Hash function allows taking input of data with independency, applying hash and then getting an output that proves that a delta change in input gives a uniquely different output. The output is termed as digest. These are a few properties are as follows; *1)Preimage (or inverse image) resistant:* By the term itself we understand that given a particular output we can never find an input for it. Thus, it is difficult to get *ahash(x)* if a direct is specified. *2)Second Preimage Resistant:* This property prevents security issues as well. Thus, for any given input we cannot find another input having the same output such that getting a hash(x) = hash(y) is an infeasible process if viewed from a logical computational perspective. *3)Collision Resistant*: This property verifies further more that no two inputs can hash to a same digest output.Maximum block chains are implemented using Secure Hash Algorithm having digest size of 256 bits or 32 bytes (SHA – 256). SHA – 256 makes the system collision resistant since to match any two inputs to the same digest the algorithm has to be worked out at a minimum of 2128 times. Hence, cryptographic hash functions give immense security to the entire block chain system.

Cryptographic Nonceis [3] an abstract number added in the hash input along with the data which itself gives a different digest even if the two data inputs are same but nonce is different. *Hash (data + nonce) = digest.*

2.1.IMMUTABILITY

Immutability means changeless. Blockchain Technology is immutable means the data present in the blocks can't be altered. By using combined form of cryptography and blockchain hashing process we make this technology immutable. There are some process through which this trait is reversed like 51% attack, Quantum computing etc. In present day the blockchain is used mostly in field of crypto currencies. Through 51% attack, users or attackers can reverse their transaction and again spend it. So, it is also said as "Double spend". To perform this, user require high hashing process and computing power.The strength of blockchain depends on the length of the chain. As many users involve in a chain, the length of the chain becomes longer and stronger because the copy of the ledger is distributed among all the users. By making the corrupted longest chain one can perform this process. It consumes a lot of electricity and power resources, whose cost is very high and makes this operation unrealistic. By using permissioned blockchain formula, the network can be secured from this attack.To do transaction in blockchain user need private keys and public keys [4]. Quantum computing has the ability to hack the cryptography hash function and get the private key.

ISSN: 2582-3167 (online)

IRO Journal on Sustainable Wireless Systems (2020)
Vol.02/ No. 1
Pages: 13-22
http://irojournals.com/irosws/
DOI: https://doi.org/10.36548/jsws.2020.1.002

2.2.BLOCKCHAIN GOVERNANCE

"Blockchain does not come under anyone" This is not strictly true. In permissioned blockchain, routine users don't have the allowance to add block in the chain. They only do the transaction. But there are some exclusive user and developers of that blockchain have the permission to create and publish new blocks. A fixed amount is awarded to that person. The whole control and governess is driven by member of the associated owner or consortium. Permission less blockchain networks are often governed by blockchain network users, publishing nodes and software developers. Each group has a level of control that affects the direction of the blockchain network's advancement. Strategies on which Blockchain is governed:-

1) In Benevolent Dictator for life, the final decisions which are in the favour of blockchain are taken by the owner of that blockchain.

2) In Core development team, if users demands special features in the blockchain, only core development team has the power to take decision on what is or is not going to be included in the official release [5]. Under core development team there are two groups-

Core developers are the group responsible for maintaining the code that underpins the blockchain software itself. They can't put it into effort because they don't control the network itself.Node operators are those people in the chain who have all the rights to run the blockchain software and maintain the full copy of ledger. The only work of node operator is to decide whether to implement code change in their node.

3) In open chain governance strategies, the developers or core team makes the list of some decision and present it in front of users, the system's users have to select one of them and this decision is finalized.

2.3.INTEGRATION OF BLOCKCHAIN AND IOT

Blockchain is mainly used for transferring crypto currency from one account to another and data stores publicly with the cryptographic hash encryption. But nowadays many parcel shipping companies like FEDEX are accepting this technology to provide transparency in their shipping methodology, provide a secure server to do online payments and secure their payment card details. If we only introduce blockchain into these type of companies challenges like users can't track the route of parcel, not able to see whether the parcel is being shipped or not, and if only IoT is used problems likes 1) Resource optimization where device in IoT are not suited for high level and complex security method, 2) not so much adequate to provide privacy to user's diverse types of data, 3) single point of failure, many-to-one traffic and reduce scalability of an operation if centralized server for IoT is used [6]. To get out from these trouble BCoT (The blend of blockchain and internet of things framed as blockchain of things) is introduced.

Key features of BcoT:

1) *Decentralisation and autonomy* – within blockchainIoT devices are connected to each other, so all the data are shared and contained within the single network, so managing the entities becomes easy. it violets the rule of single point failure.

ISSN: 2582-3167 (online)

IRO Journal on Sustainable Wireless Systems (2020)
Vol.02/ No. 1
Pages: 13-22
http://irojournals.com/irosws/
DOI: https://doi.org/10.36548/jsws.2020.1.002

2) *Cost reduction* – all the data are distributed among the users so it take low space and IoT devices communicate without a large server system [7]. There is no role of middlemen and intermediaries.

3) Many features of blockchain like resilient, distributed peer-to-peer systems and the ability to interact with peers in a trustless and auditable manner is also applicable here. Smartcontracts allow us to automate complex multi-step processes. By the integration of Blockchain and IoT we accelerate our workflows in very unique way, reduce the time consumption and provide immutability by achieving cryptographic verifiability.

3.CASE STUDIES

1) Case study of Bitcoin:

It follows P2P network system where files are secured cryptographically. There is no need of trusted third parties. So, it minimizes the cost of transaction.To prevent the coin from double spend, instead of making a central server system ,bitcoin introduce "Timeserver stamp". It is a hash function include the hash of previous block. Bitcoin use hash cash. Proof of Work system which is easy to verify by honest nodes but difficult to crack it. On increasing the block the work increases and protects the block from getting tempered. To programme the rate of adding block in the chain, difficulty level of proof of work is set. Nodes always follow longest chain. It use SHA-256 mechanism to give high security to a file, where a 256 bit (32 bit) hash function is produced by giving an input. But it can't be reversed.

To do a transaction bitcoin and other crypto currencies deduct a small amount of fees and these fees are used to maintain blockchain network and pay as reward to nodes for adding new block in the network act as an incentives to be honest for that network. To avoid introducing new coin and reversing the transaction amount by attackers ,nodes in the networkneed more computational power in comparison to the attacker's power. Bitcoin goes through Markle root system, in which there is a hash function of separate transaction. By combination of two hashes a new hash formed, so there is a necessity of even no of transaction .if there is an odd no transaction then hash cloned itself and make new hash code. .in the last a hash is generated in result of all transaction and combine with the previous block's hash to give a unique hash code to that block.

2) Case study of Block Chain in Microsoft

Microsoft has quietly been building bridges between its blockchain services and other, widely used infrastructure and platforms, such as Office 365 Outlook, SharePoint Online, Salesforce, Dynamics 365 CRM Online, SAP, and even Twitter, according to Matt Kerner, the general manager of Microsoft Azure [8]. The idea is to allow Microsoft customers to port their data from these platforms into the cloud, and from there onto a blockchain. In addition to the usual blockchain efficiencies, one of the less-discussed benefits of distributed ledger technology (DLT) in a cloud environment like Azure, according to Microsoft, is that it amasses data from multiple companies in a standardized format at scale. The potential to mine data for all sorts of insights then becomes limitless, the company reckons. Hence, the company is integrating tools such as Microsoft Flow and Logic Apps – which offer hundreds of connectors to thousands of applications – into Azure Blockchain Workbench, a service it launched in May to make the creation of blockchain apps easier (Workbench currently has Ethereum Proof of Authority configured as the consensus

ISSN: 2582-3167 (online)

IRO Journal on Sustainable Wireless Systems (2020)
Vol.02/ No. 1
Pages: 13-22
http://irojournals.com/irosws/
DOI: https://doi.org/10.36548/jsws.2020.1.002

protocol). Cloud computing enabled departments within the same company to break out of their data silos and collaborate on heterogeneous data sets, increasing smarts through machine learning (ML) and artificial intelligence (AI). Stepping back, many would argue that data is now the most valuable naturally occurring resource on the planet. As the race to prove the best data analytics intensifies, firms are springing up whose sole purpose is to structure and format data to run AI algorithms on but with enterprise blockchain, you get the structured and formatted data part quite easily.

3) Block Chain in IBM

IBM Blockchain is a public cloud service that customers can use to build secure blockchain networks. The blockchain is a notion that came into the public consciousness around 2008 as a way to track bitcoin digital-currency transactions. At its core blockchain is a transparent and tamper-proof digital ledger. Just as it could track bitcoin's activity in a secure and transparent fashion, it's capable of tracking other types of data in private blockchain networks [9]. This could allow any private company or government agency to set up a trusted network, which would allow the members to share information freely, knowing that only the members could see it, and the information couldn't be altered once it's been entered. The company is offering a set of cloud services to help customers create, deploy and manage blockchain networks. This fits in with IBM's broader strategy to offer a wide range of cloud services to its customers. Although the blockchain piece is based on the open source Hyperledger Fabric project of which IBM is a participating member, it has added a set of security services to make it more palatable for enterprise customers, while offering it as a cloud service helps simplify a complex set of technologies, making it more accessible than trying to do this alone in a private datacenter. While the work these companies have done to safeguard blockchain networks, including setting up a network, inviting members and offering encrypted credentials, was done under the guise of building extra safe networks, IBM believes it can make them even safer by offering an additional set of security services inside the IBM cloud. IBM claims their blockchain product is built in a highly auditable way to track all of the activity that happens within a network, giving administrators an audit trail in the event something did go awry. The company has been testing a consumer digital identity network built on top of the IBM blockchain technology with banks in Canada. If it works as advertised, it could end up greatly simplifying and securing how we maintain and share our identities in a digital context, allowing us to expose only the information the requesting authority requires (and no more), while enabling us to revoke those sharing privileges at any time. Take the example of an online document service like Evernote or Google Docs.

Ethereum, would return control of the data in these types of services to its owner and the creative rights to its author. Only the user can make changes, not any other entity. In theory, it combines the control that people had over their information in the past with the easy-to-access information that we're used to in the digital age. Each time you save edits, or add or delete notes, every node on the network makes the change.

4) Case study of FEDEX

FEDEX, an American multinational delivery service, also revealed plans to join block chain technology. During an interview, they revealed that they want to provide the information about the supply chain to their customers. Block chain is giving even more visibility to the customers about the packages before it gets in their hands and after it leaves

ISSN: 2582-3167 (online)

IRO Journal on Sustainable Wireless Systems (2020)
Vol.02/ No. 1
Pages: 13-22
http://irojournals.com/irosws/
DOI: https://doi.org/10.36548/jsws.2020.1.002

their hands [10]. They will be having millions of records a day so, to secure those records they want to integrate block chain technology, so that all the data exchange will takes place in a very secure way. The role of block chain is the ledger of block chain will record and store all the information about your package.

The information includes:

1) The price you paid
2) The expected date for shipping
3) The actual date of shipping
4) The expected arrival date
5) The actual arrival date and time

The block chain will secure all this data and the data cannot be changed without your knowledge.
The block chain will be combined with AI and IOT sensors, a block chain tracking system can be accurately trace the origin of products and verify the authenticity of everything

5) Case study of Ripple

Ripple is nothing but a real time currency exchange, gross settlement system ad remittance network. Ripple depends on a common standard ledger, which stores information about all accounts of ripple [11]. Ripple have its own currency and also allows everybody to use their own currency via RIPPLE NET. RIPPLE NET:-Ripple net is a network which is mostly used by payment providers like banks....etc. these institutions will use the solutions of ripple to provide frictionless experience to send money globally. The Ripple net will work at a minimal commission of $0.00001.the only reason for not being free is to prevent the attack of DDOS Distributed denial of service (DDOS) attack:

It is an attack in which multiple compromised computer systems attack a target, website or any other network resources and causes some effect of service for users of targeted resource XRP: XRP is the currency of ripple. The main purpose of XRP is to intermediate in between two different currencies. P2P system- abbreviation is peer to peer network system. This is a decentralized network allow the user to access others system files within the network, if the file is publically shared.

6) Case study of Ethereum

Ethereum is one of the newest technologies to join this movement. Ethereum has the goal of using a blockchain to replace internet third parties — those that store data, transfer mortgages and keep track of complex Financial instruments. Ethereum wants to be a 'World Computer' that would decentralize the existing client-server model [12]. With Ethereum, servers and clouds are replaced by thousands of "nodes" run by volunteers from across the globe. The vision is that Ethereum would enable this same functionality to people anywhere around the world, enabling them to compete to offer services on top of this infrastructure. Scrolling through a typical app store, for example, one

ISSN: 2582-3167 (online)

sees a variety of colorful squares representing everything from banking to fitness to messaging apps. These apps rely on the company (or another third-party service) to store your credit card information, purchasing history and other personal data – somewhere, generally in servers controlled by third-parties. Your choice of apps is of course also governed by third parties, as Apple and Google maintain and curate (or in some cases, censor) the specific apps you're able to download.

4.CONCLUSION

In this paper the importance of Blockchain technology which is used to set a new protocol to information security and authentication has been extensive covered with different real time scenarios and examples. From the case studies done on most high rated companies like IBM, Microsoft, Fedex, Ripple and Ethereum it can be concluded that IBM has devised a very powerful and most efficient Blockchain protocol since the While the work these companies have done to safeguard blockchain networks, including setting up a network, inviting members and offering encrypted credentials, was done under the guise of building extra safe networks, IBM believes it can make them even safer by offering an additional set of security services inside the IBM cloud. IBM claims their blockchain product is built in a highly auditable way to track all of the activity that happens within a network, giving administrators an audit trail in the event something did go awry. Thus there is lots of research going on in the field of integration of IoT with Blockchain to enhance security. Our future work would be to integrate IoT and Blockchain for development of Smart meters for smart cities.

REFERENCES

[1] Dylan Yaga, Peter Mell, Nik Roby, Karen Scarfone, "Blockchain Technology Overview", October 13, 2018, NIST Interagency/Internal Report (NISTIR) – 8202 https://doi.org/10.6028/NIST.IR.8202

[2] Arif Sari, " Use of Blockchain in Strenghtening Cybersecurity and Protecting Privacy" , Internation Journal of Engineering and Technology, vol. 2 , pp.59-66, December 2018

[3] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System Cryptography Mailing list, March 24, 2009, http:// metzdowd.com,

[4] Konstantinos Christidis, Michael Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things" Department of Electrical and Computer Engineering, North Carolina State University, Raleigh, NC 27606, USA Corresponding

[5] Miraz M.H. (2020) Blockchain of Things (BCoT): The Fusion of Blockchain and IoT Technologies. In: Kim S., Deka G. (eds) Advanced Applications of Blockchain Technology. Studies in Big Data, vol 60. Springer, Singapore

[6] E. Monsing, J. Mather, and S. Moura. Blockchains for decentralized optimization of energy resources in microgrid networks. In Conference on Control Technology and Applications (CCTA),pages2164–2171.IEEE, 2017.

[7] Yakubov,A.;Shbair,W.M.;Wallbom,A.;Sanda,D.;State,R.A blockchain-based PKI management framework. In Proceedings of the NOMS 2018—2018 IEEE/IFIP Network Operations and Management Symposium, Taipei, Taiwan, 23–27 April 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 1–6.

[8] https://azure.microsoft.com/en-in/solutions/blockchain/

[9] https://www.ibm.com/blockchain/what-is-blockchain

ISSN: 2582-3167 (online)

IRO Journal on Sustainable Wireless Systems (2020)
Vol.02/ No. 1
Pages: 13-22
http://irojournals.com/irosws/
DOI: https://doi.org/10.36548/jsws.2020.1.002

[10] https://blockchainflashnews.com/how-fedex-is-benefiting-from-blockchain/
[11] https://www.investopedia.com/terms/r/ripple-cryptocurrency.asp
[12] https://www.genesis-mining.com/what-is-the-ethereum-blockchain

ISSN: 2582-3167 (online)