International Journal of Computer Techniques -– Volume 7 Issue 2, April 2020

RESEARCH ARTICLE OPEN ACCESS

A Review of Usability and Security Evaluation Model ofBlockchain Technologies

PallabBanerjee[1] ,Biresh kumar[2] , Amarnath Singh[3] ,Harsh Prasad[4] , Bittu Raj[5]

[1,2,3]*Assistant Professor,Dept. Of Computer Science & Engineering, Amity University, Jharkhand.*
[4,5]*B.TechScholar,Dept. Of Computer Science & Engineering, Amity University, Jharkhand.*
Email: pbanerjee@rnc.amity.edu

-------------------------------------***********************--------------------------------

Abstract:

In the modern trends of evolution Blockchain has received extensive attention recently. In the race of digitalization, the world is looking on the technology that can fuel financial transaction significantly, Thus Blockchain provide such types of facilities. As we know, Blockchain is a decentralized peer-to-peer network which was designed in order to remove involvement of third party in transaction. But due to its extensive use on a large scale there is huge problem of security and scalability.This paper aims to provide a review of Usability and Security of some of blockchain Technology on different categories: Public, Consortium and Private on different application Model such as Smart contract, Internet of Things and Crypto- currency considering different parameters. This paper basically provide a comparative study and coordination between them. We also expand to provide a typical consensus algorithm comparison which governs the blockchain.

Keywords —**Blockchain, Decentralized, Scalability, Usability.**

-------------------------------------***********************--------------------------------

1. Introduction

Blockchain is a open distributed ledger that can permanently record transaction between two parties efficiently in the network and the data in the given blocks cannot be altered without alteration of all subsequent blocks, which requires consensus of the network majority. It consist of a single universal ledger where every block added in linked with the last block which has its own hash value for inter connected network. Current blockchainsystem are categorized into three types: public blockchain, consortium blockchain and private blockchain. In public blockchain there is no access restrictions, anyone with the network connection can join and participate in the execution of consensus protocol. As, for consortium blockchain is a partial decentralized system which is granted to a group of approved individuals. In case of private blockchain its most of the features are similar with public, only with a difference that is known as a permission based system, the block with read and write access are controlled by an entity.

In this paper we focused on some of the important application which is governed by the blockchain, such as **Smart contract, Internet of Things and Crypto- currency**. We also provide a comparative view on some of the most important consensus algorithms which includes **Pow, Pos, Dpos, Ripple, Poa**.

The majority of researcher are more focused on revealing and improving limitations of blockchain security and privacy but lack on understanding different categories of blockchain and its uses on different applications. We wish to stress that the purpose of our paper is not to define the working principle of blockchain technology nor its consensus algorithms rather to provide a feasible basic comparison between its application and consensus algorithms for understanding its future limitations . We hope that our paper will increase more understanding of problem at stake and motivate further study and research in this field for future development.

2.Briefing

In the table 1 as shown below we did a comparative study and analysis on some of the applications of blockchain as **Smart Contract, Internet of Things and Crypto-currency**, keeping in mind about its **Access Permission, In-commutable, Proficiency, Dominance, Litigation Perspective and Technical Failure.** All the factors have different limitations on different platform, i.e. in case of smart contract its

Property	IOT,SMART CONTRACT, CRYPTOCURRENCY	Public	Consortium	Private
Access Permission		Anyone can access/see or access.	Only selected nodes/people that are allowed to access/see.	Only particular organization can access/see.
Incomputable		It is not so easy or it may be impossible to tamper.	There is a chance to tamper.	High chances of tampering.
Proficiency/Efficiency		Not so efficient, but Best in case of (Smart Contract).	Can be efficient but not as compared to public.	As compared to other two not so efficient as it can provide advantage to particular node.
Dominance/Ownership		Nobody, Everyone has equal rights and Dominance throughout the system.	Multiple nodes/or selected people from the chain.	Single system.
Litigation Perspective		Is still a challenge, as who will bear the liability for any faults in the technical code and who has the right to enforce against them.	Is still a challenge, as who will bear the liability for any faults in the technical code and who has the right to enforce against them.	People within the system are responsible to bear for any sort of faults.
Technical Failure		Difficult to tract the bugs in the system if any system failure happens.	Bugs can be trace.	Bugs can be trace.
Timestamp		Time consuming.	Less time required.	Due to limited or restricted nodes it is very efficient in time consumption.

accessibilities are different on public, consortium or in private mode; same in case of Iot devices or crypto- currency.

Table: 1

A smart contract is just a legal digital contract with the security of the consensus protocols governed by blockchain that automatically get executed when the defined terms andconditions of the contract are met successfully without alteration. A Cryptocurrencies are the group of tokens which are used within blockchain networks to send value and pay transactions without the need for a central authorization. When IoT and Blockchain come together, smart devices will be able to exchange data and communicate with one another through a decentralized system of blockchain where there will no longer be any dependence on a centralized authority.

3.Consensus Efficiency:

As we know blockchain is governed by some of the major algorithm and the basic contract for fulfillment of the goal. In this paper we compared these listed popular algorithms and provided a comparative study of its contract in different forms of blockchain as shown in the table 2.

Statements:

Pow: Proof-of-Work: It is an algorithm which is use to provide the authentication of the data in the network. Itstime consuming approach provide difficulty in operation but an easy verification and authentication of the node that is added in the chain.

Pos: Proof-of-Stake**:** Is a low energy consumption consensus algorithm for locking up crypto assets to secure the network which require nodes to purchase or receive the coin and commit it to authenticate the transactions.

Dpos: Delegated-Proof-of-Stake: It is bit similar to Pos only with a difference thatits technology is maintained through democratic voting procedure to secure blockchain network.

PROPERTY	POW	POS	DPOS	POA	RIPPLE
Energy Efficiency	Not at all efficient. Consume most of the power in computation work.	Less as compared to Pow	Same as Pos	Efficient	Efficient
Network Maintenance	It can deters denial-of-service attacks and other service abuse.	It provide network tokens by locking them to produce and approve networks.	It provide the efficient democratic version of the procedure Pos mechanism	Pre-selected authorities provide security. They are very scalable and adjusted to be a platform for decentralized App. development.	It has a continuous security procedures, in which(PPCA) is applied every sec by all nodes. .
Adversary Power of Properties	More than 25% computing power	More than (50+1)% stake	More than (50+1)% validator	1/3rd of faulty node.	More than 15-20% faulty node
Implementation / Example	Bitcoin based crypto – currencies such as LITECOIN	PEERCOIN	LISK,STEEM, WAYKICHAIN, BITSHARE	MICROSOFT AZURE	RIPPLE

Table: 2

Poa: Proof-of-Authority: This algorithm is basically used for comparatively fast transaction through mechanism based on on identity as a stake. As with the help of POA, nodes earn the right to become validators to retain the position that they have gained.

Ripple: Is a real-time peer-to-peer decentralized algorithm for settlement which provide platform for a seamless transfer of money in different format

4. Conclusion

Blockchain is witnessing a major demand in a public sector which includes Banking, Insurance, Logistics, Healthcare and Public- Administration, etc. For basic implementation of blockchain we need to understand its advantage and limitations so that they can be utilized effectively in differentplatforms.In this paper, we gave an overview of important application which is governed by the blockchain, such as Smart contract, Internet of Things and Crypto-currency.with respect to Public, Consortium and Private blockchain. We have alsoprovided a typical consensus algorithm comparison which governs and coordinates the blockchain.We believe that this paper will open up many research challenges in resource sharing on blockchain and its applications on different platforms.

Acknowledgement

All thanks must be sent to the management of Amity University Jharkhand (AUJ) and its team of Computer Science Departmentto facilitate accessing the resources used in this study.

References

[1]M.Knecht and B. Stiller, "Smartdemap: A smart contract deployment and management platform," in IFIP International Conference onAutonomous Infrastructure, Management and Security, pp. 159–164,Springer, 2017.

[2]V. Buterin, "A next-generation smart contract and de-centralized application platform 19/07/2018.

[3]M. Alharby and A. van Moorsel, "Blockchain-based smart contracts: A systematic mapping study," arXiv preprint arXiv:1710.06372, 2017.

[4]S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security,privacy and trust in internet of things: The road ahead," Computer Networks, vol. 76, pp. 146–164, 2015.

[5] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," Computer Networks, vol. 57, no. 10, pp. 2266–2279,2013.

[6]Kitchenham B, Charters S. Guidelines for performing Systematic Literature Reviews in Software Engineering;2007.

[7]Coinmarketcap, Crypto-Currency Market Capitalizations; 2016.Accessed:24/3/2016.

[8]Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electroniccash system." Consulted1.2012(2008):28.

[9] M. Vukolić, "The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication," in International Workshop on Open Problems in Network Security, Springer, 2016, pp. 112–125.

[10] I.-C. Lin and T.-C.Liao, "A Survey of Blockchain Security Issues and Challenges," Int. J. Netw.Secur., vol. 1919, no. 55, pp. 653–65901, 2017.

[11] J. Barcelo, "User privacy in the public bitcoinblockchain," 2014.

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

[13] G. Maxwell, "Coinjoin: Bitcoin privacy for the real world," in *Post onBitcoin Forum*, 2013.

[14] T. Ruffing, P. Moreno-Sanchez, and A. Kate, "Coinshuffle: Practical decentralized coin mixing for bitcoin," in *Proceedings of European Symposium on Research in Computer Security*, Cham, 2014, pp. 345–364.

[15] I. Miers, C. Garman, M. Green, and A. D. Rubin, "Zerocoin: Anonymous distributed e-cash from bitcoin," in *Proceedings of IEEE SymposiumSecurity and Privacy (SP)*, Berkeley, CA, USA, 2013, pp. 397–411.

[16] E. B. Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza, "Zerocash: Decentralized anonymous payments from bitcoin,"in *Proceedings of 2014 IEEE Symposium on Security and Privacy (SP)*,San Jose, CA, USA, 2014, pp. 459–474.

[17] "Crypto-currency market capitalizations," 2017. [Online].Available:https://coinmarketcap.com

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

[19] S. King and S. Nadal, "Ppcoin: Peer-to-peer crypto-currency with proofof-stake," *Self-Published Paper, August*, vol. 19, 2012.

[20] "Bitshares - your share in the decentralized exchange." [Online]. Available: https://bitshares.org/

[21] D. Schwartz, N. Youngs, and A. Britto, "The ripple protocol consensus algorithm," *Ripple Labs Inc White Paper*, vol. 5, 2014.

[22] F. Tschorsch and B. Scheuermann, "Bitcoin and beyond: A technicalsurvey on decentralized digital currencies," *IEEE Communications SurveysTutorials*, vol. 18, no. 3, pp. 2084–2123, 2016.

[23] 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

[24] D. Lee KuoChuen, Ed., *Handbook of Digital Currency*, 1st ed.Elsevier, 2015.[Online].Available:http://EconPapers.repec.org/RePEc:eee:monogr:978 0128021170

[25] G. Foroglou and A.-L.Tsilidou, "Further applications of the blockchain,"2015.

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