Blockchain Technology

Aakash Jain[1], Ms. Neeraj Kumari[2]

CCSIT, TMU, MORADABAD

[1]aakashjain2710@gmail.com

[2]neeraj.computers@tmu.ac.in

***Abstract*—**

The main aim of Paper is to provide a brief summary of Current scenario of Blockchain technology in the information technology. This paper will provide a reference of technological aspects and working principal of blockchain technology. In today's world blockchain has already become an emerging technology and a lot of researches and revolution has just began regarding this blockchain technology. Although, the most popular Cryptocurrency since it has been invented is Bitcoin also, it is the best example of blockchain technology. Since, it was invented there are other cryptocurrency too like Ethereum, Monero, Litecoin, Dogecoin etc. Which are using this technology In this paper we will be discussing about the research and experiments being done on this blockchain technology .The paper also gives a short introduction of various analysis of blockchain use case.it will help us to understand necessary aspects of developing blockchain technology.

***Keywords*— Bitcoin, Blockchain, distributed ledger, use case.**

I. INTRODUCTION

In the cutting edge universe of innovation, now and again another innovation rises that is by all accounts the response to the majority of our issues and appears to start the start of another brilliant. Since 2016 blockchain has been the said flash, despite the fact that the primary form was at that point acknowledged in 2008[1] and the nuts and bolts were incepted by Haber and Stornetta as of now in 1991[2]. The name is as of now self-clarifying as blockchain comprises of squares, which are included in a steady progression, much the same as in the renowned round of "wind". from an utilitarian point of view it fills in as decentralized database without focal expert, it utilizes TCP/IP convention so as to impart between P2P organize individuals, or as it were it is a framework that works in a manner as to give exact and irreversible information exchange to decentralized P2P network[2].

One of the main pragmatic arrangement with the utilization of blockchain is cryptographic money bitcoin[3],[2]. Whose esteem has officially grown multiple times since it surfaced, and started the notoriety of the blockchain to its present statures? This is additionally a bad mark since usually mistook for bitcoin, and the majority of the investigations are centred around bitcoins blockchain, in spite of the fact that there are innumerable varieties and subtleties. A precedent the extent of papers on blockchain to the papers on bitcoin is at about 4:1 proportion and the mind lion's share of research today is centred around taking out the impediment of blockchain from private resources and security viewpoint and not on investigating its conceivable application out of esteem recording scope [4]. The same number of creators [5]-[7] show, at present blockchain is viewed as an achievement innovation, which could change the day by day timetable and business forms in various application areas, for instance, to record the quantity of votes in a decision, and guarantee straightforwardness in bookkeeping, track the property tights of extravagance things, protected innovation rights, and so on.

II. BLOCKCHAIN IN THEORY AND PRACTICE

A. Related Work

Blockchain is a very recent research and still there is no in-depth research conducted so far in the area. There are different researches and different publications are taking place in different forums or blogs. As an original paper written by Satoshi Nakamoto [1] was published on internet in his vlogs but it was never reviewed as an proper Scientific research paper even it didn't had the term Blockchain. There are numerus numbers of research paper available over the internet but most of them are trying to exploit popularity of various cryptocurrency and are nothing other than compilation of different Bitcoin description. In 2016 Bitcoin and technologies was written by Narayanan and it was published by Princeton university[2] and it was made with serious studies and it can be further used for various studies. This describes principals and foundation of blockchain technology and its application in different real-life use cases. But all researches and its mentoring indicates need for further research in the field. Many others believe that blockchain has significant potential, even though there is lot of obstacles and challenges in real life implementation. But there are lot of significant potential but still there is a a lot of challenge for real life implementation. For example, there is none of the single worldwide acceptable

definition of blockchain; so it has become a necessary to develop a common standard and regulation both legal and technical. If a reasonable employment is required then it is necessary to formulate and develop unified approach in blockchain technology.

B. Definition of Blockchain

There is an assortment of definitions by various creators and as pointed out in [15], there is no single, universally concurred definition: so it is critical to comprehend the essential ideas of blockchain. A few people are of the view that blockchain isn't yet characterized legitimately [16]: thusly, they use bitcoin as a kind of perspective point and utilize the fundamental three points-exchanges, accord, and system. Hileman and Rauchs[3] offer definition, where appropriated record is characterized as an a sort of dispersed database that can have 'hinders' with transactions and is sending all information to all hubs in its system . Tama et al. [17] are of same point of view, saying that blockchain is a "part of the usage layer of an appropriated programming framework", whose reason for existing is to guarantee information respectability.

Concurring to[18] the answer for including another record, approving and dispersing the data over P2P arrange. A few creators disregard more insights concerning blockchain and spotlight on information honesty just, for example,[19] states that blockchain is basically a cryptographically unquestionable rundown of datay.

A standout amongst the most ideal ways on characterizing blockchain is by choosing highlights, without which the essential standards of blockchain would never again be unmistakable. By doing this task it is conceivable to state that blockchain is an information structure with the accompanying key components [20]:

- data redundancy (each node has a copy of the blockchain);
- check of exchange prerequisites before approval;'
- recording of exchanges in successively requested hinders, whose creation is led by an accord calculation;
- Exchanges dependent on open key cryptography and an exchange scripting language.

Discussion in regards to meaning of blockchain turns out to be particularly imperative when managing legitimate issues, for example, going of new laws to characterize the utilization of blockchains. As Jeffris[22] calls attention to, expansive contrasts in definitions may cause eccentric issues sooner rather than later as the administration passes enactments with respect to blockchain. Presently a portion of the nations (Estonia, Switzerland, Arizona, in the U.S.) have set up the essential legitimate structure of blockchain in which its definition is likewise included. Walch[23] and Stark[24] have made an authoritative research in regards to definitions and law, where it is appeared most subjects, who are responsible for passing blockchain related enactment, chiefly do it to demonstrate its crypto benevolent nature, yet the nature of the innovation is very slacking. Taking everything into account, it is to be seen that blockchains can have a wide assortment of practically extraordinary types [25] in this manner, one definition won't generally be versatile to all cases. In any case, in any depiction of blockchain its key focuses ought to be incorporated for example to store information and give trust in their legitimacy.

C. Main Features of Blockchain

As the name recommends, blockchain is a chain of squares. Typically each square comprises of a hash pointer, which is a connection to the following square. In such degree that it is difficult to erase any square or supplement another one amidst a square chain, since then hashes won't be indistinguishable. Squares are made by system members, who are handling the exchange to blockchain a hub must determination a hash capacity of the square that fulfils certain scientific conditions[26], in spite of the fact that standards of square appending can be extraordinary and can rely upon a separate accord calculation, which is utilized in a specific blockchain.

For a square to be implanted in a chain, an accord must be come to. It suggests that all members in a system must affirm its genuineness. By relying upon specialized parameters, a square is incorporated into a chain after a specific number of conditions are affirmed, anyway, it is being approved by the majority of the hubs on a system, until everybody has an exceptional blockchain structure. Some studies [2] consider a proof of work agreement as a fundamental development from Satoshi Nakamoto's blockchain, which is known as bitcoin. Precisely this instrument replaces the focal specialist and gives motivators keeping all system individuals fair.

Agreement can be come to from multiple points of view, which is reliant on the specialized methodology utilized. As blockchain is an appropriated framework, at that point accord is partitioned [27]. This implies a higher level of trouble as a result of the variables; for example, arrange dormancy, accidents and conceivable noxious system members. In [2] it Is referenced that regardless of hypothetical challenges and a high probability of disruption, current use of conveyed accord are working stunningly better than they ought to have regardless of whether there is no experimentally demonstrated clarification for that.

Another essential piece of blockchain innovation is information appropriation. Again it tends to be freak in view of the recently portrayed availability parameters. Blockchains can utilize established information dissemination models and

every ha consistant preferences and disadvantages, which must be painstakingly evaluated against the planned objectives. For instance shared information appropriation will be less solid however it will offer more prominent decentralized and subsequently better security against conclusion of system. Appropriated frameworks can likewise accomplish more noteworthy computational power by going along with it by the clients yet it accompanies an expense of damage that can be brought about by vindictive clients. However, it accompanies cost of conceivable harm done by vindictive clients [17].

D. Main Risks of Blockchain

Conceivable outcomes dependably join dangers. Each canter capacity of blockchain has a few huge dangers that need to be assessed and counter estimated before execution. Not generally these dangers will be simply specialized, in light of the fact that dangers can likewise emerge from lawful, efficient, even social territories.

One of the fundamental concerns with respect to decentralized systems is constantly about their control (see likewise [29]). For instance, blockchains with a proof-of-work agreement calculation are hypothetically helpless against the purported 51-percent assault, when one system hub would have 51 % of complete system computational power, along these lines picking up probability to without any help affirm exchanges and make new squares [2].

There is dependably chance in such kind of advances as each centre capacity of blockchain has a few huge dangers that should be assessed and executed before counter estimation. Fundamentally dependably these dangers will be absolutely specialized it very well may be from legitimate, affordable, and might be social zones. A standout amongst the most celebrated model in history of blockchain is the alleged "DAO wars".

The DAO signifies “Decentralised Autonomous Organisation”, although Dao was first Etherium-based blokchain. During mid- 2016 someone found a loophole in this DAO and used this vulnerability and used it to transfer 56 Million $ [30]. After this incidence blockchain got spilt into different branches scientifically termed as Etherium forked. Due to this maximus network participant stopped continuing support for Etherium.However some part of Etherium blockchain was continued to function and was termed as Etherium Classic. Lack of academic research and security is another reason of Security risk.

After all there is a wide scope of danger of utilizing digital currency. Then again the utilization of RSA and ECC are for the most part viewed as protected yet at the same time there is plausibility to find obscure up and coming weakness or secondary passages.

III. BLOCKCH AIN APPLICATION IN DIFFERENT AREAS

During early 2016 Blockchain gained recognition in wider no. of audience, it led to significant increment in proposed service and application software, which is completely based on blockchain.it, is very important that investors and others too should understand limitations of blockchain. In recent years it has been seen that There are numerous attempts of using blockchain is taking place in financial sector. It happened due to Bitcoin and several other cryptocurrencies. Which have open a way for rest of the world.

As estimated by Hileman & Rauchs[3] 30% of use case of blockchain is related to banking and financial services. While other sectors such as government (13%), insurance (12%) and healthcare (8%) is being related to blockchain. As it has been seen that all the sectors are using it as on initial stages of adaptation cycle and the expectations are very inflated. It will take several more years for fully implementation as it depends on the experimental stage.

Table I beneath presents a rundown of some known programming applications and use cases, where blockchain has been utilized as one of the fundamental parts (Table I, altered and incorporated from the accompanying sources: [2], [3], [8], [12], [13], [18]). Rundown isn't to be viewed as total, since it is preposterous to expect to accumulate data pretty much all current use cases. Because of quick blockchain improvement, new arrangements additionally seem every day.

The table underneath is expected to give an outline and general thought regarding the most famous arrangements that are utilized at present. Some of them are still just at the testing stage; consequently, full usefulness is absent. Order of utilization cases into classifications is just for simpler diagram and isn't to be considered as official arrangement. Some of blockchain specialists would contend that all exercises identified with blockchain are information recording and permanent stockpiling [16]; in this manner, increasingly nitty gritty gathering is pointless, however it makes more enthusiastically to see significance of each utilization case.

Table 1
BLOCKCHAIN USE CASES

Category	**Applier**	**Use case**
Data Mangemnt	Eris, Mastercoin Chromeway	Network infastructure
	Swarm	Content & resource distribution
	Peernova Maidsafe	Cloud Storage
	Modum.io	Data monitoring
	Etherium Symbiont	Contract Mangement
	Multichain	Inter-organisational Data mangement
	UniquID,SolidX Microsoft,IBM ShoCard	Identity Data Mangement
	Factom, Securechain	Tamper-proof event Log and audit trail
	Blockstack	System metadata storage
	DataBrokerDAO Filament,Chimera	IoT sensor data Purchasing
Data Verification	Uproov	Photo And video proofing
	Bitcourt, Blocksign	Document Notarisation
	APPII	Work history Varifiacation
	Sony global Education	Acadmical certification
	Microsoft, Everpass	Product Quality Verification
	Artplus, Tierion	Proof of origin
Financial	Barclays, BNP Paribas	Trade Finance
	Karken,Bitstamp Coinbase	Currency Exchange
	Bitbay, Bitbond	P2P Payments
	Waves ,Starbase	Crowdfunding
	Insurechain	Insurance
	Chain	Stock Share and bond issuing
	Sweden(on idea Level	Central bank Money issuing
	Eaterra,profeth	Supply chain mangement
	Ripple,Zcash Bitcoin,Litecoin	Value transfer And lending
Other	Augur,Gnosis	Prediction Recording
	Thanks Coin	Social Voting System
	Arcade City LA'Zooz	Ridesharing
	NAmecoin	Domain name Registration
	DNA bits, Medicare	Healthcare record storing
	IBM	Software Licence validation
	Po.et, Nexus Group	Content or product timestaping
	Lastis,Etherpot	Lottery
	Chroma Wave BitLand	Property right Registration
	SOMA	Social rating monitoring
	Europian Parliament	Voting in elections
	Borderless.Tech	Marriage registration
	PrecedentCoin	Court Proceedings
	SETI@home, Folding@home	Computional power outsourcing for scientific purpose
	Slock it	Electronic locks
	TransActive Grid	Electro energy selling
	Blockverify	Product tracing
	Playcoin,DeckBound	Gaming
	TRST.im,Asimov	Reviews & endorsement

IV. CURRENT RESEARCH IN EVALUATION OF BLOCKCHAIN

It is necessary to perform at least a short analysis of proposed solution feasibility in case of considering different application

of blockchain and use case, because quiet often it happens the scientific paper or article just describes only theoretical description and doesn't have any clear idea of physical implementation. Many start-ups are often trying to attract investors rather than creating useful and helpful solutions. In 2017 ICO known as initial coin offering gained a popularity as it was launching various tokens and cryptocurrency coin and were often viewed as scams by serious investors.

There has been Attempt of concentrating on ICOs in 2018 preceding propelling any coins.it is normal that as ICO is getting prevalent it will encourage more inquires about in this specific region and lead to exacting assessment models.To outline conceivable and severe assessment of blockchain reasonableness for record-keeping ,a system is utilized by Lemieux which decides climate information records are reliable or not and whenever found right and precise then a point by point clarification of structure and piece is pursued.

V. CONCLUSION

This Paper has provided a concept and overview of the maximum numbers of currently existing and known use cases with blockchain technology. Use cases has been taken and compiled from various different sources, such as industry expert blogs, scientific papers, research papers, master thesis and research, this paper has limited scope, therefore, a list of mentioned use case not to be considered exhaustive. From the review of various use cases of blockchain application is used by financial sector. In this paper a brief and basics of blockchain application has been provided. it is worth mentioning that research and inventions in blockchain evaluation model is still at early stage, and thus, Further research in this area is very necessary. By applying strict and correct evaluation of blockchain necessity can save large number of resources in software development and research cost.

REFERENCES

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf [Accessed: 8 May 2018].

[2] Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, Bitcoin and Cryptocurrency Technologies. Princeton University Press, 2016, 308 p.

[3] G. Hileman & M. Rauchs, Global Blockchain Benchmarking Study. Cambridge, United Kingdom: Cambridge Centre of Alternative Finance, Sept. 2017. Available: https://ssrn.com/abstract=3040224 [Accessed: 8 May 2018].

[4] D. Yang, J. Gavigan, and Z. Wilcox-O'Hearn, Survey of Confidentiality and Privacy Preserving Technologies for Blockchains, 2016. Available: https://www.r3.com/wp-content/uploads/2017/06/survey_ confidentiality_privacy_R3.pdf [Accessed: 8 May 2018].

[5] Citi Group. [Online]. Citi GPS: How FinTech is Forcing Banking to a Tipping Point, March 2016. Available: https://www.citivelocity.com/citigps/ [Accessed: 3 May 2018]

[6] Everis NEXT, "17 Blockchain Disruptive Use Cases," 31 May 2016. [Online]. Available: https://everisnext.com/2016/05/31/blockchain-disruptive-use-cases/ [Accessed: 8 May 2018].

[7] R. Krawiec, D. Housman, M. White, M. Filipova, F. Quarre, D. Barr, A. Nesbitt, K. Fedosova, J. Killmeyer, A. Israel, and L. Tsa, Blockchain: Opportunities for Health Care. NIST Workshop on Blockchain & Healthcare, Aug. 2016. Available: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/public-sector/us-blockchain-opportunitiesfor-health-care.pdf [Accessed: 8 May 2018].

[8] M. Conoscenti, A. Vetro, and J. C. De Martin, "Blockchain for the Internet of Things: A Systematic Literature Review," in IEEE/ACS 13th International Conference of Computer Systems and Applications, 2016, pp. 1–6. https://doi.org/10.1109/AICCSA.2016.7945805

[9] "Survey on Establishing Evaluation Model for Blockchain," Mitsubishi Research Institute, 2017. Available: http://www.meti.go.jp/meti_lib/report/H28FY/000346.pdf [Accessed: 8 May 2018].

[10] P. Zhang, D. C. Schmidt, J. White, and G. Lenz, "Metrics for Assessing Blockchain-Based Healthcare Decentralized Apps," in IEEE 19th International Conference on e-Health Networking, Applications and Services, 2017 pp. 17–20. https://doi.org/10.1109/HealthCom.2017.8210842

[11] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," in IEEE 6th International Congress on Big Data, June 2017,pp.557–564. https://doi.org/10.1109/BigDataCongress.2017.85

[12] N. Bauerle, "What are the Applications and Use Cases of Blockchain?". [Online]. Available: https://www.coindesk.com/information/applicationsuse-cases-blockchains [Accessed: 8 May 2018].

[13] K.Christidis and M. Devetsikioti, "Blockchains and Smart Contracts for the Internet of Things," IEEE Access, vol. 4, pp. 2292–2303, 2016. https://doi.org/10.1109/access.2016.2566339

[14] BitFury Group and J. Garzik, "Public versus Private Blockchains — Part1: Permissioned Blockchains, Part2: Permissionless Blockchains, 2015. Available: http://bitfury.com/docs/

[15] V. Lemieux, Blockchain Technology for Record Keeping: Help or Hype?, vol 1. University of British Columbia, 2016. Available: https://www.researchgate.net/profile/Victoria_Lemieux [Accessed: 8 May 2018].

[16] H. Okada, S. Yamasaki, and V. Bracamonte, "Proposed Classification of Blockchains Based on Authority and Incentive Dimensions," in 19th International Conference on Advanced Communication Technology, 2017. https://doi.org/10.23919/ICACT.2017.7890159

[17] B. A. Tama, B. J. Kweka, Y. Park, and K. H. Rhee, "A Critical Review of Blockchain and Its Current Applications," in International Conference on Electrical Engineering and Computer Science, 2017, pp. 109–113. https://doi.org/10.1109/ICECOS.2017.8167115.

[18] A. Lewis, "So You Want to Use a Blockchain for That?," Jul. 2016. [Online]. Available: https://www.coindesk.com/want-use-blockchain/ [Accessed: 8 May 2018].

[19] H. Halpin and M. Piekarska, "Introduction to Security and Privacy on the Blockchain," in 2nd IEEE European Symposium on Security and Privacy Workshops, 2017. https://doi.org/10.1109/EuroSPW.2017.43

[20] S. Porru, A. Pinna, M. Marchesi, and R. Tonelli, "Blockchain-Oriented Software Engineering: Challenges and New Directions," in IEEE 39th International Conference on Software Engineering Companion, May 2017, pp. 169–171. https://doi.org/10.1109/ICSE-C.2017.142

[21] T. Swanson, Consensus-as-a-Service: A Brief Report on the Emergence of Permissioned, Distributed Ledger Systems. R3 CEV, 2015

[22] A. Jeffries, "'Blockchain" is Meaningless," The Verge, March 2018. [Online]. Available: https://www.theverge.com/2018/3/7/17091766/ blockchain-bitcoin-ethereum-cryptocurrency-meaning [Accessed: 8 May 2018]

[23] A. Walch, "The Path of the Blockchain Lexicon (and the Law)," 36 Review of Banking & Financial Law 713, 2017. Available: https://ssrn.com/abstract=2940335 [Accessed: 8 May 2018]

[24] J. Stark, Applications of Distributed Ledger Technology to Regulatory and Compliance Processes. R3, 2017. Available: https://www.r3.com/ wp-content/uploads/2017/07/apps-reg-compliance_R3.pdf [Accessed: 8 May 2018].

[25] V. Buterin, "On Public and Private Blockchains," Aug. 2015. [Online]. Available:https://blog.ethereum.org/2015/08/07/on-public-and-privateblockchains [Accessed: 8 May 2018].

[26] H. Vranken, "Sustainability of Bitcoin and Blockchains," Current Opinion in Environmental Sustainability, vol. 28, pp. 1–9, 2017. http://doi.org/10.1016/j.cosust.2017.04.011

[27] L. S. Sankar, M. Sindhu, and M. Sethumadhavan, "Survey of Consensus Protocols on Blockchain Applications," in 4th IEEE International Conference on Advanced Computing and Communication Systems. https://doi.org/10.1109/ICACCS.2017.8014672

[28] K. Croman, C. Decker, I. Eyal, A. Gencer, R. Wattenhofer et al. "On Scaling Decentralized Blockchains," in International Financial Cryptography Association: FC 2016 Workshops, 2016, LNCS 9604, pp.106–125.Available: http://fc16.ifca.ai/bitcoin/papers/CDE+16.pdf [Accessed: 8 May 2018].

[29] S. Azouvi, M. Maller, and S. Meiklejohn, "Egalitarian Society or Benevolent Dictatorship: The State of Cryptocurrency Governance," in 22nd International Conference on Financial Cryptography and Data Security, March 2018. Available: https://fc18.ifca.ai/bitcoin/papers/ bitcoin18-final13.pdf [Accessed: 8 May 2018].

[30] F. Hofmann, W. Simone, E. Ron, and M. Böhmecke-Schwafert, "The Immutability Concept Of Blockchains And Benefits Of Early Standardization," in ITU Kaleidoscope: Challenges for a Data-Driven Society, Nov. 2017. https://doi.org/10.23919/ITU-WT.2017.8247004.