A Survey on Blockchain Technology & Future Scope

Vinay Srivastava
M.Sc in Computer Science,
University of Guelph, Guelph, Canada

***Abstract*—** Blockchain Technology had the foremost impact on our lifestyles within the last decade. many of us still confuse Blockchain with Bitcoin, however they're not a similar. Bitcoin is associate application that uses Blockchain technology. However, as a distributed technology blockchain as a robust tool may be used for Brobdingnagian way of life applications. There's a large spectrum of blockchain applications starting from cryptocurrency, risk management, net of things (IoT), monetary services to public and social services. Blockchain technology has shown its wide ability in recent years as a spread of market sectors need ways in which of integration its potentials into their operations. Blockchain has ton of advantages like decentralization, determination, obscurity and auditability. Though variety of studies specialize in usage of blockchain technology in numerous application aspects, there's no comprehensive survey on the blockchain technology in each the technological and application views. To fill this gap, we have a tendency to conduct a comprehensive survey on blockchain technology, blockchain sort, reviews blockchain application and technical challenges. Moreover, this paper additionally points out the longer term side of blockchain technology.

***Keywords*—** Blockchain, Smart Contract, Cryptocurrency, IoT, Security, Digital Ledger, PoW, PoS.

I. INTRODUCTION

Blockchain, although unnamed as such at that point, was introduced to the world in a whitepaper, in 2008, its utilisation in the advanced shared money framework, Bitcoin. Bitcoin is a type of organisation convention, similar to HTTP or TCP layers, which supports worldwide web framework and utilised each time we peruse the worldwide Web. A blockchain is a record of advanced exchanges, it is decentralised and not heavily influenced by any individual, gathering or organisation. The blockchain technology is organised and it is difficult to change the guidelines or its substance without the agreement among the individuals who are utilising it. In blockchain more up-to-date impedes are connected to the more seasoned ones, shaping a chain, subsequently the term blockchain. This structure guarantees that lone the passages can be included information base, information can never be changed or taken out because changing a solitary section in a more established square would mean modifying the whole history of exchanges resulting to that block. All the more explicitly, blockchain is an unchangeable, shared record of companion peer exchanges put away in a computerised record which is made from connected exchange blocks. Blockchain, is a technology that safely keep up persistently developing arrangements of information records and exchanges. Blockchain depends on set up methods of cryptography to permit every one of the members of an organisation to cooperate for store, trade, and view data. In a blockchain framework, there is no brought together position; rather, than it, exchange records are put away and dispersed over the organisation. Above all, all information passages are stepped with date and time. Associations with the blockchain medium become known to all members and require confirmation by the organisation before adding the data, empowering trust less joint effort between network members while recording an unchangeable review trail of the obvious multitude of communications. For security, clients can refresh just the square to which they have the entrance, and those updates get reproduced over the organisation. Blockchain, though not named per se at the time, was conferred to the planet during a whitepaper, in 2008, its use within the digital peer-to-peer currency system, Bitcoin. Bitcoin could be a variety of network protocol, like HTTP or protocol layers that underpin international web infrastructure and used on every occasion we have a tendency to browse the planet Wide internet. A blockchain could be a ledger of digital transactions, it's suburbanized and not beneath the management of anyone, cluster or company. The blockchain technology is structured and its extraordinarily troublesome to vary the principles or its content while not the agreement among the those who square measure victimisation it. In blockchain newer blocks square measure coupled to the older ones, forming a sequence, so the term blockchain. This structure ensures that solely the entries is intercalary in information, information will ne'er be changed or removed as a result of dynamic one entry in AN older block would mean revising the complete history of transactions after that block. additional specifically, blockchain is AN permanent, shared record of peer-to-peer dealingss keep during a digital ledger that is formed from coupled transaction blocks. Blockchain, could be a technology that firmly maintain

unceasingly growing lists of knowledge records and transactions. Blockchain depends on established techniques of cryptography to permit every of the participant during a network to move for store, exchange, and examine data.In a blockchain system, there's no centralized authority ; rather than it, dealings records square measure keep and distributed across all the network. most significantly, all information entries square measure sealed with date and time. Interactions with the blockchain medium become well-known to any or all participants and need verification by the network before adding the knowledge, enabling trust less collaboration between network participants whereas recording AN permanent audit path of all the interactions. For security functions, users will update solely the block to that they're having the access, and people updates get replicated across the network. Bitcoin is that the terribly 1st application of blockchain, it's a form of digital currency supported blockchain. thanks to the success of Bitcoin, individuals currently will utilize blockchain technologies in several field and services, like money market, IOT, offer chain, election balloting, medical treatment, document handling and pursuit in office, insurance pursuit record and cybercriminals. We use these tools or services in our way of life, cybercriminals and cybercrime may be eradicated through this blockchain technology. Despite the actual fact that the blockchain technology has nice potential for the development of the longer term web systems, it's facing variety of technical challenges. Firstly, measurability could be a immense concern. Bitcoin block size is proscribed to 1MBnowand a block is mined regarding each ten min. later, the Bitcoin network is restricted to a rate of seven transactions per second, that is incapable of coping with high-frequency commercialism. However, larger blocks mean larger cupboard space and slower propagation within the network. this can result in centralization bit by bit as users would love to keep up such an oversized blockchain. so the exchange between block size and security has become a challenge. Secondly, it's been tried that miners can do larger revenue than their fair proportion through ungenerous mining strategy (Eyal and Sirer, 2014). Miners hide their mined blocks for additional revenue within the future. therein manner, branches will surface frequently; this hinders blockchain development. therefore some solutions got to be advocate to repair this drawback. Moreover, it's been shown that privacy outflow may happen in blockchain even once users solely build transactions with their public key and personal key (Biryukov et al., 2014). User's real informatics address might even be caterpillar-tracked. what is more, current agreement algorithms like proof of labor (PoW) or proof of stake (PoS) face some serious issues. for instance, prisoner of war wastes an excessive amount of electricity energy whereas the development that the made get richer might seem within the PoS agreement method. These challenges got to be self-addressed within the blockchain technology development. In this paper, we are going to have a fast study regarding blockchain theory, key options of blockchain technology, completely different application in blockchain, distinction form of services and security & privacy problems that we want to beat.

II. THE THEORY OF BLOCKCHAIN

Blockchain technology is not using one single technique but contains Cryptography, mathematics, Algorithm and economic model, combining peer-to-peer networks and using distributed consensus algorithm to solve traditional distributed database synchronization problem. The following six key elements of blockchain are:

A. Decentralized

Blockchain doesn't have to rely on centralized node anymore, the data can be recorded, stored and updated distributively.

B. Anonymity

Blockchain technologies solve the faith problem between one node to other node, so data transfer can be unidentified, only person's blockchain address need to know.

C. Autonomy

The blockchain solely works according to the rules which are defined by its members. There is no central-authority for the defined rules.

D. Automation

Manual processes that are generally guided by the legal contracts can be automated with a self-executing type of computer program called as smart contract. A smart contract is a component of a blockchain-based system which can automatically enforce stakeholder-agreed rules and process steps. Once launched, smart contracts are completely unidentified; when the conditions of contracts are met, prespecified and agreed actions occur automatically.

E. Security

There are various ways which proves a blockchain is more secure than other record-keeping systems. Transactions must be agreed upon before they are recorded into the system. Once a transaction is approved, it is encrypted and then linked to the previous

transaction. This, along with the fact that information is stored across the network of computers instead on a single server, makes it very difficult for hackers to compromise the transactional data. In any trade wherever the protection of sensitive information is crucial — money services, government, care — blockchain has a chance to vary however the vital data is shared by helping to prevent frauds and unauthorized activity.

F. Transparency

The data's record by blockchain system is transparent to each node, it is also transparent on update of data that is why blockchain can be trusted. Changes to public blockchains are publicly viewable by all parties creating transparency, and all transactions are unchangeable.

III. TYPE OF BLOCKCHAIN ARCHITECTURE

There are different kinds of blockchain architecture, each of them have different design and architecture.

A. Public Blockchain

In such blockchain, everybody in the organisation can approve the exchange and can partake during the time spent achieving agreement. It guarantees decentralisation by setting up a square of distributed exchanges. Every exchange is joined with the blockchain before it goes to the framework. Subsequently, it very well may be affirmed and adjusted with each hub in the organisation. Anyone with a PC and web association can be selected as a hub and can be given the total blockchain history.It states that everyone can check the exchange and confirm it, and can likewise partake during the time spent getting agreement. The advantage of the public organisation is the secrecy of the client and full straightforwardness of the record.

B. Private Blockchain

Node will be restricted, not every node can participate in this blockchain, has harse authority management on data access. Private blockchains have a stern management with respect to the authority of the data access in the network. None of the nodes in the network can participate in the verification and validation of transactions. Instead, a company or organization initiates, verifies and validates each transaction. This gives a higher level of efficiency in the verification and validation of transactions. The benefit of private blockchain is that a company can select the access rights to individuals and permit a higher level of privacy when compared with public blockchains. A private blockchain is suitable to a traditional and governance model based business. Using a privately-run version of blockchain can bring the organization into the current century. Private blockchains are more prone to acceptability by the private sector or government based companies as they allow a central authority to be present with a more secure, more efficient and faster technology.

C. Consortium Blockchain

Consortium blockchain is a combination of public and private blockchain and can be interpreted as partly decentralized. These blockchains are open to public but not the entire data is available to all the participants. User rights vary and blocks are validated based on the predefined rules. Consortium blockchains are hence "partly decentralised". Consortium Blockchains are the ones in which the consensus process is controlled by a preselected set of trusted nodes. A block is added to the chain after consensus is achieved through the transaction validation by a group from the preselected set of nodes. In a consortium Blockchain, the right of reading the blockchain can be public or made restricted only to participants. In addition to this, consortium Blockchains are considered to be partially decentralized unlike private Blockchains. A consortium blockchain model is more appealing to corporate companies, because of the fact that it is decentralized unlike private Blockchains.

IV. APPLICATIONS OF BLOCKCHAIN TECHNOLOGY

A. Internet of Things (IoT)

In an IoT biological system [40], the greater part of the correspondence is as like Machine-to-Machine (M2M) cooperation. Hence inaugurating trust between the partaking machines is that the major challenge that IoT innovation still has not been met wide. Nonetheless, Blockchain might set about as associate degree impetus in such manner by empowering upgraded ability, security, dependableness, and confidentiality. This can be accomplished by conveying Block chain innovation to follow billions of gadgets associated with the IoT eco-frameworks and used to empower and additionally arrange the exchange processing. Relating Block chain within the IoT circle can likewise build reliability by surgical operation the only purpose of Failure (SPF). The cryptologic calculations used for cryptography of the block info even as the hashing strategies might provide higher security. In any case, this will request all the more processing force which IoT gadgets presently experience the ill effects of. In this manner, supplementary investigation is obligatory to defeat this contemporary restriction. A portion of the instances of block chain IoT are

1. Smart Appliances
2. Supply Chain Sensors and so on.

Specifically, the blockchain may well be extraordinarily helpful in building the safety safeguarding IoT. A privateby- structure IoT may well be inspired by the consolidation of the block chain besides a P2P stowage framework.

B. Finance

- Financial services. The emergency of blockchain systems like Bitcoin (Nakamoto, 2008) and (hyperledger, 2015) has brought an enormous impact on ancient monetary and business services. Blockchain has the potential to disrupt the globe of banking. Blockchain technology may well be applied to several areas together with clearing and settlement of monetary assets etc. Besides, showed that there square measure real business cases like collateralisation of monetary derivatives that would leverage blockchain to cut back prices and risks.
- Enterprise transformation. In addition to the evolution of monetary and business services, blockchain will facilitate ancient organizations to complete the enterprise transformation swimmingly. Consider an example of postal operators (POs). Since ancient communication operators (POs) act as an easy negotiator between merchants and customers, blockchain and cryptocurrency technology will facilitate POs to increase their straightforward roles with the availability of new financial and un-financial services.
- Risk management. Risk management framework plays a major role in monetary technology (FinTech) and currently it may be combined with blockchain to perform higher. Pilkington (Pilkington, 2016) provided a unique risk-management framework, during which blockchain technology is employed to analyse investment risk within the Luxembourgish situation. Investors who nowadays hold securities through chains of custodians tend to face the risk of any of these failings.

C. Smart Contracts

- **Blockchain Healthcare.** Individual Health records may well be encoded and placed with a personal key on the blockchain with a personal key which might allowance the admittance solely to the specific individuals. The similar system may well be utilised to ensure that the exploration has been conducted through HIPAA (secure and secret) legislation. Surgery receipts could be kept on a blockchain and sent naturally to protective suppliers as proof of transportation. The ledger, as well, could be utilized for human services, for example, administering drugs, direction consistency, testing results, as well as overseeing the medicinal services supplies.
- **Blockchain Music.** Key problems in the music business include ownership rights, distribution of royalties and simplicity. The sophisticated music industry focuses on monetizing productions, while ownership rights are frequently disregarded. Innovation in blockchain and smart contracts can address this problem by creating a comprehensive and precise decentralized music rights database.
- **Food Safety.** One more captivating usage for blockchain could be in the outlining nourishment from its inception to your plate. Along these lines, the block chain data is changeless; you'd have the ability to pursue the vehicle of wherewithal things from their motivation to the store. In addition, ought to there be a nourishment-borne ailment; block chain would enable the wellspring of the pollutant to be originate significantly snappier than it tends to be now.

V. SECURITY AND PRIVACY OF BLOCKCHAIN

Securityideas and principles are listed below:

A. Defense in Penetration

This is a strategy which uses numerous corrective measures to protect the data. This principle of protection of data in multiple layers is more efficientthan single security layer.

B. Minimum Privilege

In this strategy data access is reduced to the lowest level possible to reinforce elevated level of security.

C. Manage vulnerabilities

In this strategy we check for vulnerabilities and manage them by identifying, authenticating, modifying and patching.

D. Manage Risk

In this strategy we process the risks in an environment by identifying, assessing and controlling risks.

VI. CHALLENGES OF BLOCKCHAIN

A challenge can be defined as an implicit demand for proof. Some of the major challenges currently faced by blockchain technology are listed as below.

A. Scalability

With regular volume growth of blockchain utilization and therefore the come the sheer range of exchanges on a daily basis, the blockchain is ending endlessly stupendous in size. All transactions are stored in each and every node to get validated. The current transaction should be validated first before the other transactions to be validated. The restricted block size and the time

interval used to create another block plays an important part in not fulfilling the requirement of processing millions of transactions simultaneously in real time scenarios. Meanwhile, the size of the blocks in blockchain may create an issue of transaction delay in the event of little transaction, as diggers transaction fees, miners would prefer to validate transactions. As referenced in, the proposed solutions for the adaptability issue of blockchains can be categorized in two classes: storage optimization and redesigning of blockchains.

The database would keep up rest of the non-empty addresses. A customer with light weight could likewise be utilized as another to fix the versatility issue. In updating, the blockchain can be divided into a key block and a smaller scale block, with the key block responsible for leader elections while the micro block responsible for transaction storage.

B. Privacy Leakage

The blockchain is mainly vulnerable to transactional privacy leakage due to the fact that the details and balances of all public keys are visible to everyone in the network.

The proposed solutions for accomplishing anonymity in blockchains can be extensively classified into mixing solution and anonymous solution. Mixing is a service that offers anonymity by transferring assets from numerous info delivers to various yield addresses.

C. Selfish Mining

Selfish mining is another challenge faced by blockchain. A block is susceptible to cheating if a small portion of hashing power is used. In selfish mining, the miners keep the mined blocks without broadcasting to the network and create a private branch which gets broadcast only after certain requirements are met. In this case, honest miners waste a lot of time and resources while the private chain is mined by selfish miners.

D. Personal Identifiable Information

Personal Identifiable Information (PII) is any information that can be used to remove an individual's identity.

E. Security

Security can be discussed in terms of confidentiality, integrity and availability as discussed in [19]. It is always a challenge in open networks such as public blockchains.

Confidentiality is low in distributed systems that imitate info over its network Integrity is that the metier of blockchains though there exists several challenges. Availability in blockchains is high in terms of readability thanks to wide replication compared to write down handiness. The 51% majority attack is more theoretical in a large blockchain network because of these properties.

F. Merit and Demerit of Blockchain Technology

The main merit of the Blockchain technology are decentralized network, transparency, trusty chain, unalterable and indestructible technology. In turn, the main demerit of the Blockchain are the high energy dependence, the difficult process of integration and the implementation's high costs.

G. Future of Blockchain Technology

According to York Solutions: By 2022, at least one innovative business built on blockchain technology will be worth $10 billion. By 2026, the business value added by blockchain will grow to just over $360 billion, then by 2030 grow to more than $3.1 trillion.By 2022, at least one innovative business built on blockchain technology will be worth $10 billion. By 2026, the business value added by blockchain will grow to just over $360 billion, then by 2030 grow to more than $3.1 trillion.

VII. CONCLUSION

The blockchain, additionally referred to as distributed ledger technology, is actually a digital information managed by a redistributed system, consisting of variety of various computers, in part of one centralized server. These completely different computers area unit noted as nodes and every one of them area unit connected in a very randomised approach. It is a journal which is practically difficult to produce It is extraordinarily thought of and approved for its redistributed set-up and peer-to-peer identity. Nevertheless, varied forms of analysis round the blockchain area unit safeguarded by Bitcoin. In any case, it is critical to reminder that blockchain and Bitcoin isn't a similar object. In this article, we've got surveyed the ideas of the blockchain technology, that consists of basic definitions, characteristics, key ideas, advantages, limitations, agreement algorithms and in conjunction with security challenges and the future work. We shall take associate thorough exploration of good accept the long run which includes each the centralized and decentralized models. Like any new innovation, the blockchain is a notion that originally interrupts, and over time it could endorse the improvement of a superior community that incorporates both the ancient method as well as the innovative invention.

REFERENCES

[1] I.Bentov, A. Gabizon, and A. Mizrahi, ―Cryptocurrencies without proof of work,‖ CoRR, vol. abs/1406.5694, 2014.

[2] Satoshi Nakamoto, ―Bitcoin: A Peer-to-Peer Electronic Cash System, 2008

[3] Lee R and Maeve D, ―Privacy and Information Sharing‖, Pew Research Center, 2016

[4] A.Narayanan and J. Clark, Bitcoin's Academic Pedigree, Communications of the ACM Magazine, vol. 60, no 12, Dec. 2017, p 36-45.

[5] RJ Krawiec et. al., Blockchain: Opportunities for Health Care, Deloitte Report, Aug. 2016. https://goo.gl/y423dT (Erişim: 1 Şubat 2018).

[6] Guy Zyskind, Oz Nathan and Alex 'Sandy' Pentland, ―Decentralizing Privacy: Using Blockchainto Protect Personal Data‖, Security and Privacy Workshops (SPW), 2015 IEEE [02] Satoshi Nakamoto, ―Bitcoin: A Peer-to-Peer Electronic Cash System‖, 2008

[7] Azaria A, Ekblaw A, Vieira T, Lippman A. MedRec: using blockchain for medical data accessand permission management. International Conference on Open and Big Data (OBD). Vienna, Austria: IEEE; 2016:2530 Satoshi Nakamoto, ―Bitcoin:

[8] A Hou, ―The application of blockchain technology in egovernment in china,‖ in ICCCN. IEEE, 2017, pp. 1–4

[9] B.E.Dixon and C. M. Cusack, ―Measuring the value of health information exchange,‖ in Health Information Exchange. Elsevier 2016, pp. 231–248.

[10] J.Richardson, Ethereum vs. Hyperledger, [Online] http://goo.gl/64a3Gg [26] Wall Street Firms to Move Trillions to Blockchains in 2018, IEEE Spectrum, Sept. 2017, [Online] http://goo.gl/bhr3Ck (Erişim: 1 Şubat 2018).

[11] J.Garay, A. Kiayias, and N. Leonardos, The Bitcoin Backbone Protocol: Analysis and Applications, pp. 281–310, Springer Berlin Heidelberg, Berlin, Heidelberg, 2015.

[12] A.Gervais, G. O. Karame, V. Capkun, and S. Capkun, ―Is bitcoin a decentralized currency?,‖ IEEE Security Privacy, vol. 12, pp. 54–60, May 2014.

[13] A.Gervais, G. O. Karame, K. W¨ust, V. Glykantzis, H. Ritzdorf, and S. Capkun, ―On the security and performance of proof of work blockchains,‖ in Proceedings of ACM SIGSAC Conference on Computer and Communications Security (CCS'16), pp. 3–16, New York, NY, USA, 2016.

[14] S.Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, Feb. 24, 2013. (http://bitcoin.org/ bitcoin.pdf).

[15] E.U.Opara, O. A. Soluade, ―Straddling the next cyber frontier: The empirical analysis onnetwork International Journal of Network Security, Vol.19, No.5, PP.653-659, Sept. 2017 (DOI: 10.6633/IJNS.201709.19(5).01) 659 security, exploits, and vulnerabilities,‖ International Journal of Electronics and Information Engineering, vol. 3, no. 1, pp. 10–18, 2015.

[16] J.Singh, ―Cyber-attacks in cloud computing: A case study,‖ International Journal of Electronics and Information Engineering, vol. 1, no. 2, pp. 78–87, 2014

[17] A.S.Elmaghraby and M. M. Losavio, Cyber security challenges in smart cities: Safety, security and privacy, Journal of Advanced Research, 5 (2014), 491–497.

[18] Z.Zheng, S. Xie, H. Dai, X. Chen and H. Wang, An overview of blockchain technology:Architecture, consensus, and future trends, in Big Data (BigData Congress), 2017 IEEEInternational Congress on, IEEE, 2017, 557–564.

[19] J.Mendling, I. Weber, W. V. D. Aalst, J. V. Brocke, C. Cabanillas, F. Daniel, S. Debois, C. D. Ciccio, M. Dumas, S. Dustdar et al., Blockchains for business process management-challenges and opportunities, ACM Transactions on Management Information Systems (TMIS), 9 (2018), Article No. 4.

[20] X. Li, P. Jiang, T. Chen, X. Luo and Q. Wen, A survey on the security of blockchain systems, Future Generation Computer Systems, (2017), URL http://www.sciencedirect.com/science/article/pii/S 0167 739X17318332.

[21] F.Tschorsch and B. Scheuermann, Bitcoin and beyond: A technical survey on decentralized digital currencies, IEEE Communications Surveys & Tutorials, 18 (2016), 2084–2123.

[22] Vitalik Buterin, ―Ethereum and The Decentralized Future". Future Thinkers Podcast. 2015-04-21. Retrieved 2016-05-13.

[23] Wikipedia,―Bitcoin‖,https://en.wikipedia.org/wiki /Bitc oin.

[24] Ripple, ―RippleNet‖, https://ripple.com

[25] The Future of Blockchain Technology, https://yorksolutions.net/the-future-of-blockchain-technology/.