A Survey Paper on Blockchain Concepts, Applications and Challenges

Savitha K R[1]
Sri Siddartha Institute of Technology
Tumakuru, Karnataka

Dr. Channa Krishna Raju[2]
Sri Siddartha Institute of Technology
Tumakuru, Karnataka

Dr. M. Siddappa[3]
Sri Siddartha Institute of Technology
Tumakuru, Karnataka

Abstract: The first successful plan to build a decentralised digital currency capable of entirely irreversible transactions without the need of a reliable and streamlined third party. The blockchain idea, alongside hash-based verification of-work and public key cryptography, gives an innate component of this decentralization. Indeed, even while blockchain innovation was made to handle the electronic cash twofold spending issue without depending on a confided in outsider, it is likewise being researched and applied to take care of issues in an assortment of different fields. The fundamentals of blockchain, their applications, and challenges are all covered in this article.

Keywords: Blockchain, Digital ledger, Decentralization, Cryptocurrency, Consensus algorithm

I. INTRODUCTION:

Unlike traditional techniques, blockchain allows for peer-to-peer digital asset transfers without the use of intermediaries. While finishing an exchange across a correspondence implies without depending on a believed outsider like a monetary establishment or a bank, the blockchain idea was given the Bitcoin whitepaper to conquer the twofold spending issue [1]. The main public blockchain, which supports Bitcoin, was made in view of a particular arrangement of highlights, remarkably decentralized money and shared electronic money. As a result, it was almost impossible to tailor the Bitcoin blockchain, and it had extremely limited programmable support using the Script scripting system for other reasons. Due to this intricacy, Vitalik Buterin made the Ethereum blockchain platform [2], which incorporates an inherent Turing complete programming language that permits anyone to configure Smart contracts and run decentralized applications. On the Ethereum platform, conventions like monetary standards, character frameworks, and notoriety frameworks can be made with a modest quantity of code. With the developing fame of blockchain-based digital forms of money, versatility has become a significant concern. Scaling the volume of exchanges took care of at a specific point in time is a critical perspective in scaling blockchain [3], and while this poor transaction throughput is a known issue, remedies for it pose another challenge. The motivation behind this article is to dig profoundly into blockchain standards, types, applications, issues, and upgrades by auditing distributed work from scholarly distributions, specialized reports, and meetings. The goal of this

survey report is to give a complete and detailed reference for future early blockchain technology studies.

A. Blockchain Concepts

Blockchain is a decentralized unchangeable appropriated computerized record that is gotten with amazing encryption, copied among peer hubs in a shared organization, and utilizes agreement instruments to concede to the exchange log. A ledger is a place in accounting where all transactions relating to an entity are recorded and stored. A digital ledger can be a file on a computer, a database, or even a distributed database like blockchain, where transactions are recorded electronically.

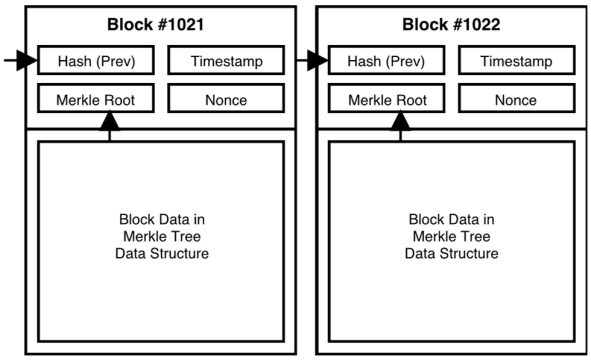

Fig 1: Common structure of blockchain

A block is made up of two parts: a header and transaction data shown in Fig 1. The block header contains four bits of information: the preceding block's hash, the time stamp, the nonce, and the Merkle tree root's hash. Changing, deleting, or editing data becomes computationally hard once a block with transactions is confirmed onto the blockchain. There are three types of networks. They are Centralized, Decentralized, and Distributed Networks. Control levels are referred to as centralization and decentralisation, while physical location is referred to as dispersion. Control is managed by a single entity in a centralised system, but control is handled by multiple independent entities in a decentralised system. A non-distributed system is housed in a single physical place, whereas a distributed system is housed in several locations.

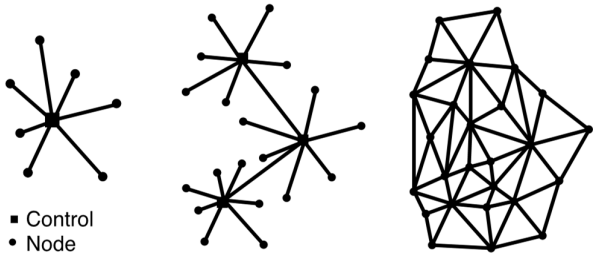

Fig 2: Different types of Networks

B. Blockchain Types

Permissionless Blockchains

Permissionless blockchains impose no limits on their nodes; anybody can openly read, inspect, and participate in the validation and publishing of data in accordance with the blockchain's consensus process. Permissionless blockchains are used by Bitcoin, Ethereum, and many other cryptocurrencies. They are also called as public blockchain.

Permissioned Blockchains

Permissioned blockchains limit the number of people who can write to a small number of people, and they use a consensus process to ensure that data is written correctly among the privileged participants. Depending upon the permissioned blockchain's necessities, the access to read could be available to anybody or locked to the public [4]. Permissioned blockchains are for the most

part utilized for corporate and social applications that require blockchain distributed ledger technology but do not require a coin to incentivize users.

II. Blockchain Application

Bitcoin

As per the underlying Bitcoin whitepaper, the essential objective of this computerized money was to give a decentralized electronic money payment component between participants by removing the need for central middlemen [5].

Ethereum

Vitalik Buterin, a cryptocurrency researcher and programmer, built a Next-Generation Smart Contract and Decentralized Application Platform. It utilizes a Blockchain-based distributed computing platform with complete Turing scripting language that allows smart contracts to be processed on the Blockchain [6].

C. Consensus Algorithms

The procedures through which hubs in the blockchain network concur on the authenticity and genuineness of exchange or information blocks are known as Consensus calculations.

Proof-of-Work

Before nodes in the network may add blocks to the blockchain, they must first solve hard mathematical one-way functions. Mining is the process of discovering proper proofs to solve cryptographic functions, and miners are the nodes or individuals who participate in it [7].

Proof-of-Stake

The algorithm in proof-of-stake selects persons known as validators to generate blocks based on a set of criteria. The standards set up how validators are picked to cast a ballot and create blocks dependent on their monetary interest in the organization, so compensating long-haul savers. [8].

Delegated Proof-of-Stake

Delegated proof-of-stake is a variation technique of proof-of-stake, in which a bunch of nodes called block producers or witnesses are chosen to produce blocks in the network. Since the quantity of block producers is limited, this system is undeniably more adaptable than proof-of-work and proof-of-stake.

Proof-of-Importance

Proof-of-importance is similar to proof-of-stake, however it doesn't rely solely on coin stake. The proof-of-importance algorithm assigns an importance score to each node, indicating its overall value to the coin's economy.

III. Application domains of Blockchain

The various application domains of blockchain technology is shown in Fig 3

A. Health care

Drug traceability and patient data management can both benefit from blockchain. In the pharmaceutical industry, drug counterfeiting is a big issue. According to reports from the Health Research Funding Organization, counterfeit pharmaceuticals account for 10% to 30% of all drugs sold in underdeveloped nations [9].

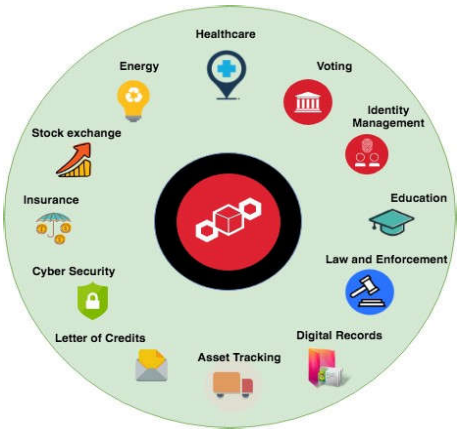

Fig 3: Various domains of applications

B. Energy Grids

Microgrids are perhaps the most well-known employments of blockchain in energy-related applications. A microgrid is a privately associated and overseen organization of electric power sources and loads fully intent on further developing energy creation and utilization efficiencies and dependability [10].

C. Stock Market

Blockchain technology has the potential to address challenges such as interoperability, trust, and transparency in fragmented market systems [11].

D. Digital Voting

Another major application that may run on an open permissioned blockchain is blockchain-based digital voting. Elections are at risk from infiltrators who can infiltrate the ballot machines, change the voter lists or databases, run fake campaigns, alter the elections reporting and more, putting the elections at risk [12].

E. Insurance

The insurance marketplace can employ blockchain to support transactions between clients, policyholders, and insurance firms. Insurance businesses can utilise blockchain to negotiate, buy, and register policies, file and handle claims, and assist reinsurance activities [13].

F. Trade Finance

Banks make the trade financing process easier by employing a letter of credit (LC) as a payment settlement strategy, which has been shown to be beneficial in risk mitigation [14].

IV. Challenges

This section describes common issues and challenges that blockchain technology faces are given

A. Performance and Scalability

When the number of transaction nodes increases in the network effects the performance concerns like throughput and latency. Although protocols like PoW provides scalability but it suffers from low throughput and high latency [15].

B. Privacy

Since the public keys are visible to all in the network, the blockchain is usually vulnerable to transactional privacy leakage. Recent research on the Bitcoin platform has revealed that a member's transaction history can be linked to identify their genuine identity [16].

C. Interoperability

Many sectors are interested in implementing blockchain technology right now. There is, however, no standard protocol that will enable them to collaborate and integrate.

D. Energy Consumption

Bitcoin's proof-of-work (PoW) algorithm allows for peer-to-peer transactions in a trust less distributed decentralised ecosystem. Miner computers, on the other hand, use a lot of electricity while doing their work [17].

E. Fairness and Security

Selfish mining [18] is another unequal way of increasing block reward in mining pools that compromises the integrity of a blockchain network. Eyal et al. fostered a blockchain network that is as yet defenceless if a humble measure of hashing power is utilized to swindle.

Future scope

Blockchain, according to the academics, has enormous promise in both academia and industry. We briefly covered many prospective applications of Blockchain technology in this part, including standardisation, asset protection, big data, and smart contracts.

Conclusion

The survey study provided a description for the blockchain and explained the principles that make up the term: peer-to-peer network, digital ledger, immutable, consensus mechanism, distributed, cryptography and decentralisation. The study also outlined the blockchain types and most extensively used consensus algorithms on blockchains for determining legitimate blocks and maintaining the blockchain's accuracy. Then we have discussed various applications domains and challenges that are faced in blockchain.

References

[1]. Nakamoto S. *Bitcoin: A peer-to-peer electronic cash system.*

[2]. Buterin V. 2013. *A next generation smart contract and decentralize application platform.*

[3]. Croman K, Decker C, Eyal I, Gencer AE, Juels A, Kosba A, Miller A, Saxena P, Shi E, Gün E. On *scaling decentralized blockchains. Lecture Notes in Computer Science. 2016;106–25.*

[4]. Vukolić M. *Rethinking permissioned blockchains. In: BCC 2017*—Proceedings of the ACM workshop on lockchain, cryptocurrencies and contracts, co-located with ASIA CCS 2017. https://doi.org/10.1145/30555 18.30555 26.

[5]. C. Decker and R. Wattenhofer, ``*Information propagation in the bitcoin network,"* in Proc. IEEE P2P Proc., Sep. 2013, pp. 1_10.

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

[7]. Gervais A, Karame GO, Wüst K, Glykantzis V, Ritzdorf H,Capkun S. *On the security and performance of proof of work blockchains.* In: Proceedings of the 2016 ACM SIGSAC conference on computer and communications security – CCS'16, 2016; 16: 3–16.

[8]. King S, Nadal S. PPCoin: peer-to-peer crypto-currency with proof-of-stake. 2012.

[9]. B. D. Glass, ``Counterfeit drugs and medical devices in developing countries," *Res. Rep. Tropical Med.*, vol. 2014, pp. 11_22, 2014.

[10]. R. H. Lasseter and P. Piagi, ``Microgrid: A conceptual solution," in *Proc. IEEE 35th Annual Power Electron. Spec. Conf.*, vol. 6, Jun. 2004, pp. 4285_4291.

[11]. L. Lee, ``New kids on the blockchain: How bitcoin's technology could reinvent the stock market," *Hastings Bus. Law J.*, vol. 12, no. 2, p. 81, 2015.

[12]. CBInsights. How blockchain could secure elections. 2018. https://www.cbins ights .com/resea rch/repor t/block chain -elect ion-security/. Accessed Aug 2019.

[13]. V. Gatteschi, F. Lamberti, C. Demartini, C. Pranteda, and V. Santamaría,``Blockchain and smart contracts for insurance: Is the technology mature enough?" *Future Internet*, vol. 10, no. 2, p. 20, Feb. 2018.

[14]. H. Har_eld, ``Identity crises in letter of credit law," *Ariz. L. Rev.*, vol. 24, p. 239, 1982.

[15]. M. Vukoli¢, ``The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication," in *Proc. Int. Workshop Open Problems Netw. Secur.* Cham, Switzerland: Springer, 2015, pp. 112_125.

[16]. R. Henry, A. Herzberg, and A. Kate, ``Blockchain access privacy: Challenges and directions," *IEEE Security Privacy*, vol. 16, no. 4, pp. 38_45 Jul./Aug. 2018.

[17]. K. J. O'Dwyer and D. Malone, ``Bitcoin mining and its energy footprint," in *Proc. 25th IET Irish Signals Syst. Conf.*, Jun. 2014, pp. 280_285.

[18]. J. Göbel, H. P. Keeler, A. E. Krzesinski, and P. G. Taylor, ``Bitcoin blockchain dynamics: The selfish-mine strategy in the presence of propagation delay," *Perform. Eval.*, vol. 104, pp. 23_41, Oct. 2016.