****

**MAEER’s**

**MIT COLLEGE OF ENGINEERING**

**PUNE - 411038**

DEPARTMENT OF INFORMATION TECHNOLOGY

**A**

**Seminar Report**

**on**

**Survey of Blockchain: Potential applications and challenges**

By

Prasad A. Pathak

(3154084)

(T150388648)

Academic Year 2017-2018

****

**MAEER’s**

**MIT COLLEGE ENGINEERING**

**PUNE - 411038**

DEPARTMENT OF INFORMATION TECHNOLOGY

# Certificate

This is to certify that Mr. Prasad A. Pathak of TE-IT-B, Seat No. T150388648, has successfully completed seminar on **SURVEY OF BLOCKCHAIN: POTENTIAL APPLICATIONS AND CHALLENGES** satisfactorily and submitted the same during the academic year 2017-18 towards the partial fulfillment of **Third Year of Engineering** in Information Technologyof **Savitribai Phule Pune University** at MIT College of Engineering, Pune.

Date :

Place :

Prof. Vaishali Suryawanshi Prof. (Dr.) A. S. Hiwale

Seminar Guide Head of Department-IT

This project based seminar report has been examined by us as per the Savitribai Phule Pune University, Pune, requirements at **MIT College of Engineering** on  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ .

(Name & Signature) (Name & Signature)

Internal Examiner External Examiner

**ACKNOWLEDGEMENT**

I take this opportunity to thank our seminar guide Prof. Vaishali Suryawanshi and Head of the Department Prof. (Dr.) A. S. Hiwale for their valuable guidance and for providing all the necessary facilities, which were indispensable in the completion of this seminar report. I am also thankful to all the staff members of the Department for their valuable time, support, comments, suggestions and persuasion. We would also like to thank the institute for providing the required facilities, Internet access and important books.

Prasad A. Pathak

**ABSTRACT**

Blockchain technologies is one of the most popular issue in recent years, it has already changed people’s lifestyle in some area due to its great influence on many business or industry, and what it can do will still continue cause impact in many places. Although the feature of blockchain technologies may bring us more reliable and convenient services, the security issues and challenges behind this innovative technique is also an important topic that we need to concern. Politics is the biggest industry there is. Democracy being a crucial element, if blockchain technologies are used to build transparent, secure, unbiased systems in every nation’s policies it would be a revolution. Such one important part of politics, voting, is taken into consideration for this project. Voting procedures have the potential to be more efficient, transparent, faster and cost effective than the one which are currently in use.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **CONTENTS**   |  |  |  |  | | --- | --- | --- | --- | | **Sr.no** |  | **Contents Name** | **Page No** | | I |  | Acknowledgement | 3 | | II |  | Abstract | 4 | | III |  | Contents | 5 | | IV |  | List of Figures | 6 | | V |  | List of Tables | 7 | | 1. |  | Introduction | 8 | |  | 1.1 | Introduction to A Secure Blockchain based Electronic Voting System | 8 | |  | 1.2 | Motivation behind A Secure Blockchain based Electronic Voting System |  | |  | 1.3 | Objective of the work |  | |  | 1.4 | Introduction to Survey of Blockchain: Potential applications and challenges |  | |  | 1.5 | Organization of the report |  | | 2. |  | Literature Survey of Survey of Blockchain: Potential applications and challenges | 10 | |  | 2.1 | Introduction |  | |  | 2.2 | Working of Blockchain |  | |  | 2.3 | Structure of Blockchain |  | |  | 2.4 | Blockchain Protocols |  | | 3. |  | Applications | 16 | | 4. |  | Challenges | 20 | | 5. |  | Conclusion | 23 | | 6. |  | Reference | 24 |   **LIST OF FIGURES** |  |  |  |

|  |  |  |
| --- | --- | --- |
| **Sr. No.** | **Figure Name** | **Page No.** |
| 1. | How Blockchain works | 12 |
| 2. | Basic structure of a Block | 13 |
| 3. | Basic structure of Blockchain | 14 |

**LIST OF TABLES**

|  |  |  |
| --- | --- | --- |
| **Sr. No.** | **Table Name** | **Page No.** |
| 1. | Comparison of Blockchain Consensus Algorithms | 8 |

**Chapter 1**

**Introduction: A Secure Blockchain based Electronic Voting System**

* 1. **Overview**

This research focused on the design of a next generation voting system built on the foundation of the blockchain. Voters expect the voting process to be anonymous, but verification of candidate tallies should be possible. Votes should be impossible to tamper with and illegitimate votes should not be counted. All vote counting would be performed in a publicly observable way. Currently a voter cannot verify his/her vote was indeed counted appropriately. Voters today are expected to ‘trust’ the polling station and voting process. When designing a new voting system, a core tenet would be to remove all need for “trust,” and place strong emphasis on open verification of the process and the votes. A similar problem was addressed with digital currency such as Bitcoin and Ethereum.

**1.2 Motivation behind A Secure Blockchain based Electronic Voting System**

The main motivation behind this project is solving the issues of digital voting by using blockchain technology and minimize problems with current voting systems. Voting should be tamper proof and all malpractices from the system should be removed with the use of technological advancements

* 1. **Objective of the work**

To build a secure, transparent, efficient voting system to replace current slow, ineffective voting systems. The final system should be unbiased and tamper proof.

**1.4 Introduction to Survey of Blockchain: Potential applications and challenges**

Blockchain is being termed as the fifth disruptive innovation in computing. In simplest words, it is a distributed ledger of records that is immutable and verifiable. Since its advent in 2008, blockchain as a concept has been used in various ways. The largest impact or application is seen as a multitude of cryptocurrencies that have sprung up. However, with time, it has become clear that blockchain as a technology is likely to have an impact much wider than just the cryptocurrency domain and much deeper than simple distributed ledger storage. This detailed survey intends to bring together all the key developments so far in terms of putting blockchain to practice. While the most common adoption of blockchain is in finance and banking domain, there are experiments being conducted by many big players in various other domains. This report will explore the various domains where blockchain has had an impact and where future implementations may be expected.

Blockchain technologies is one of the most popular issue in recent years, it has already changed people’s lifestyle in some area due to its great influence on many business or industry, and what it can do will still continue cause impact in many places. Although the feature of blockchain technologies may bring us more reliable and convenient services, the security issues and challenges behind this innovative technique is also an important topic that we need to concern.

**1.5 Organization of the report**

The following report is divided into total of six chapters. The first chapter consists of introduction to the group project topic and introduction to the seminar topic. The second chapter features the literature survey done along with working, structure and protocols of blockchain.

The third chapter of this report features the various application of blockchain and multiple industries it can potentially disrupt. This is a critical section of the report as it discusses the future possibilities in the technology industry. The forth chapter takes into account the major challenges faced by the blockchain technology. This chapter is as important as the previous chapter as it states the obstacles present in real world scenario be it political or technological limitations.

The fifth chapter presents a conclusion on the overall development on blockchain so far. The sixth chapter mentions all the references used while writing the following report, all the notable resources have been mentioned with full credit to the author.

**Chapter 2**

**Literature Survey of** **Survey of Blockchain: Potential applications and challenges**

**2.1 Introduction**

A very significant plus of the blockchain technology is that it solves two of the most dreaded problems of currency-based transactions, which have so long necessitated the requirement of a third party to validate the transactions. These are popularly known as the Byzantine Generals’ Problem and the Double Spend Problem. With advent of Blockchain, crypto economics has evolved. This very aspect has been highlighted in works of Pilkington [1]. This report explains how blockchain as a concept can be applied to a non-tokenized scheme. This report also talks about blockchain taxonomy and how hybrid solutions become an obvious choice and moving from permission less to permissioned blockchain becomes imperative to solve certain kinds of problems where trust is paramount and a public permission less ledger seems both a risk and an overhead. For a long time, the terms Bitcoin (cryptocurrency which has been the first and the most successful of the blockchain based cryptocurrencies) and Blockchain have been used interchangeably. Swan explains how these terms were used to mean one of the three things – firstly the underlying blockchain technology platform, secondly the Bitcoin protocol i.e. the software which actually runs on the Bitcoin blockchain’s network computers and makes transactions possible and thirdly the Bitcoin digital currency itself (denoted as BTC) which is the source of value. The three things listed above can be visualized as the layers of the Blockchain stack. Blockchain technology forms the lowermost layer with the Bitcoin protocol in the middle and the digital currency forming the top layer. Swan’s book [1] considers the evolution of Blockchain technology in three generations. The digital currency application is considered the Blockchain 1.0, the application of blockchain to smart contracts and Distributed Applications (DApps) is considered the Blockchain 2.0 and finally the application beyond currency and economics is detailed as the Blockchain 3.0. Peters and Panayi provide a comprehensive overview of emerging blockchain architectures, their distinction from traditional databases and role of blockchain in electronic exchanges [1].

**2.2 Working of Blockchain**

The main working processes of blockchain are as follows:

1. The sending node records new data and broad casting to network.

2. The receiving node checked the message from those data which it received, if the message was correct then it will be stored to a block.

3. All receiving node in the network execute proof of work (PoW) or proof of stake (PoS) algorithm to the block.

4. The block will be stored into the chain after executing consensus algorithm, every node in the network admit this block and will continuously extend the chain base on this block.

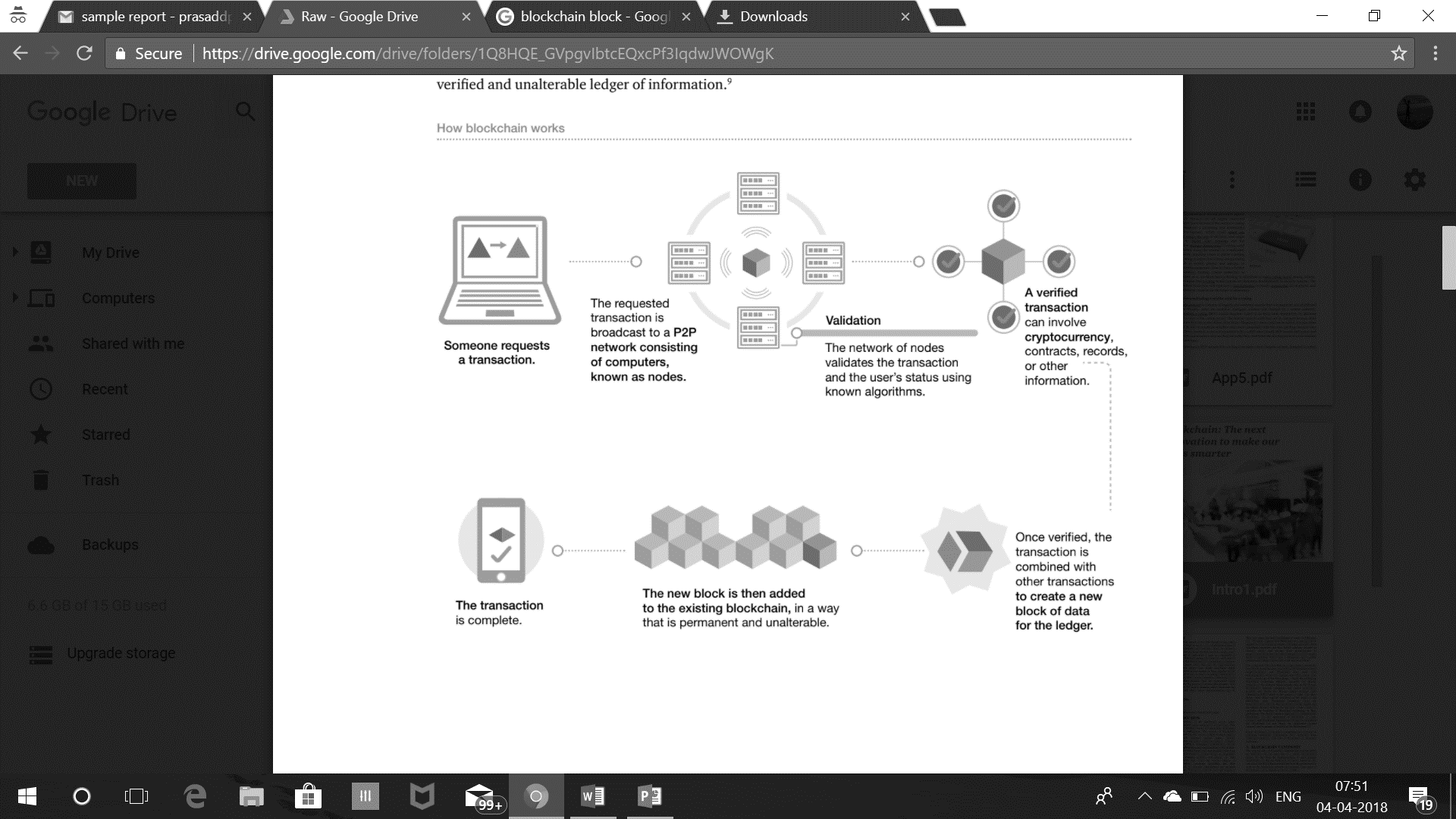


Figure 1: How blockchain works [5]

**2.3 The Structure of Blockchain**

Generally, in the block, it contains main data, hash of previous block, hash of current block, timestamp and other information. Figure 2 shows the structure of block. Main data. Depending on what service is this blockchain applicate, for example: transaction records, bank clearing records, contract records or IOT data record. When a transaction executed, it has been hashed to a code and then broadcast to each node. Because it could contain thousands of transaction records in each node’s block, blockchain used Merkle tree function to generate a final hash value, which is also Merkle tree root. This final hash value will be record in block header (hash of current block), by using Merkle tree function, data transmission and computing resources can be drastically reduced. Timestamp. Time of block generated. Other Information. Like signature of the block, Nonce value, or other data that user define.

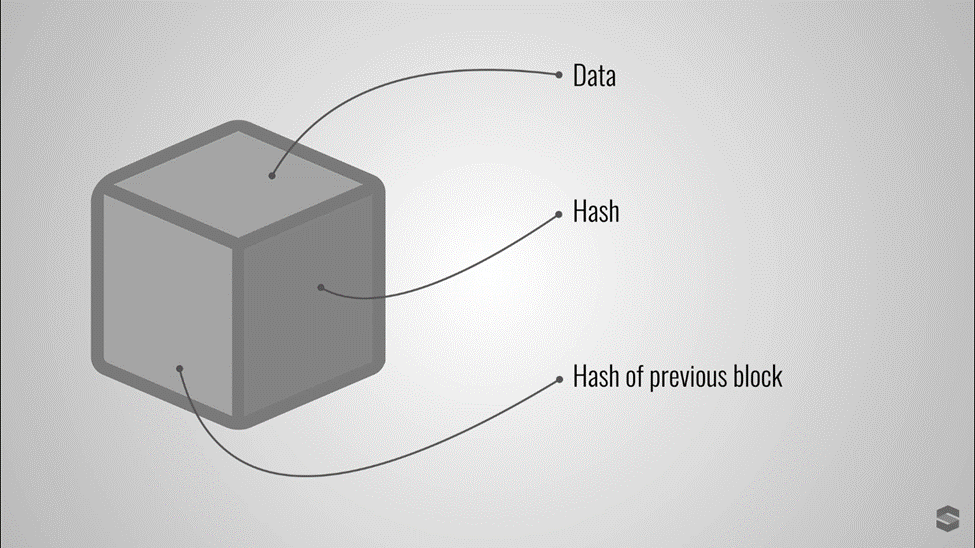


Figure 2: Basic structure of a Block

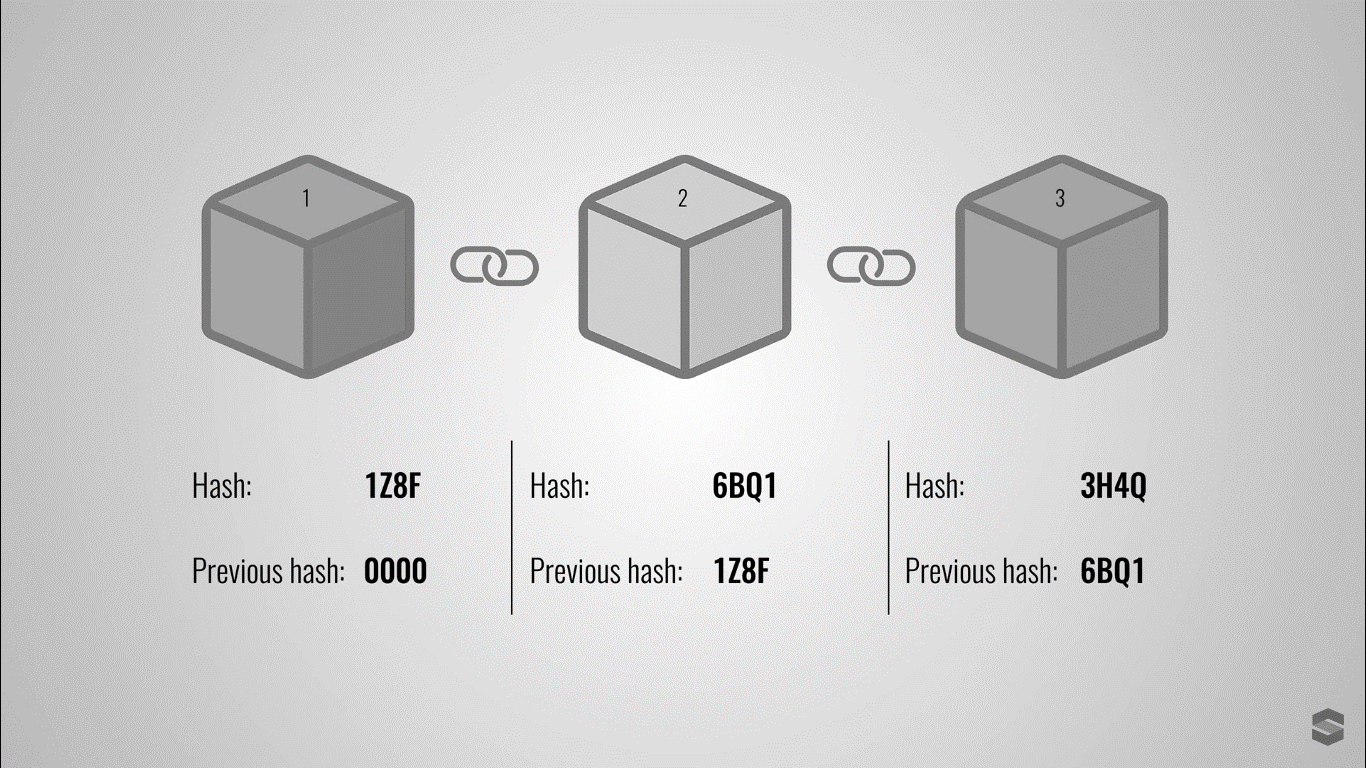


Figure 3: Basic structure of a Blockchain

**2.4 Blockchain Protocols**

Blockchain eliminates the need for third party to conduct transactions on one’s behalf. This implies that the consensus mechanism has to exist in the network itself. How a given blockchain network implements its consensus mechanism, determines the strength of the network. A foolproof consensus mechanism, suitable for purpose (of the blockchain in question) is essential to maintain sanity and coherence of data among the participating nodes of the network. The consensus mechanisms of blockchain aim to eliminate mainly two known problems with digital currency - Remove the problem of double spend and Eliminate Byzantine Generals problem. While much work has been done on blockchain protocols, there are some key algorithms explained in brief here whose variations are being used and further developed to suit various applications of blockchain. Cachin et al. [2] have explained blockchain consensus mechanism and various consensus algorithms in their research paper.

**2.4.1 Proof of Work**

PoW protocol requires all nodes on the network to solve cryptographic puzzles by brute force. For example, in case of Bitcoin blockchain, the new transactions are tentatively committed and then based on the PoW output, a selected block created by the winning node is broadcast to all the nodes, at specific synchronization intervals. Once the block is transmitted using peer to peer communication to all other nodes, the same is included in the blockchain and any tentative transactions are rolled back. By rule of probability, the consensus is achieved as 51% of power rather than 51% of people count. Effectively the computing power used by all other nodes except the winning node, is wasted [3].

**2.4.2 Proof of Stake**

Proof of stake protocol of block verification does not rely on excessive computations. It has been implemented for Ethereum and certain altcoins. Instead of splitting blocks across proportionally to the relative hash rates of miners (i.e. their mining power), proof-of-stake protocols split stake blocks proportionally to the current wealth of miners. The idea behind Proof of Stake is that it may be more difficult for miners to acquire sufficiently large amount of digital currency than to acquire sufficiently powerful computing equipment. It is also an energy saving alternative. A variation of PoS is the Delegated Proof of Stake (DPoS) algorithm. Delegated proof of stake (DPoS) is similar to PoS, as miners get their priority to generate the blocks according to their stake. The major difference between PoS and DPoS is that PoS is a direct democratic while DPoS is representative democratic. Stakeholders elect their delegates to generate and validate a block. With significantly fewer nodes to validate the block, the block could be confirmed quickly, making the transactions confirmed quickly. Meanwhile, the parameters of the network such as block size and block intervals could be tuned by the delegates. DPOS is implemented by Bitshares [3].

|  |  |  |
| --- | --- | --- |
| **ALGORITHM** | **PROS** | **CONS** |
| Proof of Work | • Considered very secure, as less prone to Sybil attack unless a mining node acquires  • 51% of the pools computing power.  • Miners get rewards (as tokens)  • Prevents unlawful forking of the chain | • Quite slow at the moment, only 1 block added in 10 mins  • Driven by rewards assigned to solving the hash, may run into problems as rewards  dwindle  • Consumes lot of electricity (mining likely to be centralized where electricity is  cheap)  • Decisions are not final till 6 blocks are confirmed |
| Proof of Stake | • Less wasteful in terms of energy consumption  • Less chance of hardware centralization  • Potentially faster than Proof-of-work protocol  • Possibly reduced possibility of selfish mining attack (assuming already rich miners are less likely to attack) | • Miners are encouraged to hold on to their stake rather than converting it into at  currency  • Economic penalties for fraudulent  attempts |

Table 1: Comparison of Blockchain Consensus Algorithms

**Chapter 3**

**Applications**

Blockchain-based applications benefit from several unique features that are not found in applications built with standard databases. Most of these features can be summarized in the following statement: it does not matter who runs a blockchain because so single entity “owns” it. What this means functionally is that data and programs stored on a blockchain will be safe against removal, and will perform accurately (as written), regardless of who is doing the work of adding new entries and archiving past ones. This is a description of an idealized blockchain system, one in which the incentives of the participants have been properly balanced but it accurately describes the most popular blockchain platforms in operation today.

Every industry stands to benefit from at least one of the features, should blockchain technology mature. Below we examine a selection of the industries that may be impacted. This list is by no means exhaustive.

**3.1 Healthcare**

The digitization of health records has brought about significant change in the public health sector, but it has been criticized for being complex on account of centralization and associated ethical issues. Blockchain technology can disrupt public health by creating a secure and flexible ecosystem for exchanging electronic health records (EHRs). This technology could also make the space more transparent by creating provenances for critical drugs, blood, organs, etc. In addition, by putting all medical licenses on a blockchain, fraudulent doctors can be prevented from practicing.

**3.2 Education**

Student records, faculty records, educational certificates, etc., are key assets in the education domain. Such records need to be shared with multiple stakeholders and it is imperative to ensure that they are trustworthy. The provenance of these records also needs to be determined accurately. Student records, faculty records and educational certificates can be maintained with the application of blockchain technology. Blockchain can also simplify certificate attestation and verification. It could even transform the manner in which the policy for educational inclusion is framed by bringing in base uniformity in the tracking of national metrics.

**3.3 Public Safety and Justice**

Blockchain could make the delivery of public safety more efficient by resolving the problem of inter-agency coordination by providing a unified source of truth that each agency independently interfaces with based on predefined conditions. Establishing a chain of custody for crucial evidence is often an important prerequisite for the evidence to be admissible; blockchain technology could help establish the provenance of the chain of custody for such evidence.

**3.4 Agriculture**

Blockchain technology can be used to increase transparency, reduce complexity and cost in food-based value chains by enabling trustworthy provenance and traceability from farmer to consumer. Other possible applications include the use of blockchain technology to record and manage agricultural land records as well as agriculture insurance.

**3.5 Civil Registration**

The civil registration process can be simplified through the application of blockchain technology to create distributed citizen registration platforms and even register vital events such as births and deaths on a blockchain. This can help make citizen records tamper-proof, resilient, secure and private, thus providing wide-ranging benefits for a variety of stakeholders.

**3.6 Defense**

Aerospace and defense companies are already moving forward in several of these areas. In examples such as tracking which individuals are certified to perform complex tasks, to understanding the authenticity of items in the supply chain, to combining blockchain identify with IoT devices, aerospace and defense companies are targeting specific proofs of concept to get started with blockchain.

**3.7 Governance**

Government departments have functional interdependence but operate in silos, which impacts the availability of services and deteriorates citizen experience. Blockchain technology can be used to break the silos, check government corruption (if any), increase efficiency and transparency. Linking file and data movement between departments through a blockchain would increase visibility into the process and ensure that the data/file moves forward in real time.

**3.8 Energy**

Blockchain technology will likely change the way that electricity is bought and sold, as well as the way that it is delivered. At the edge of the grid—where electricity dead-ends in our heaters and appliances—consumers are beginning to produce their own electricity. Blockchain technology may provide a way to incorporate these new players into the market, perhaps with the creation of open, distributed energy trading platforms. Blockchain platforms will also likely take some role in replacing the systems that now manage the distribution of electricity. As a smarter grid is built, blockchains may aid in facilitating dynamic signaling between producers and consumers, especially as the line between those roles continues to blur.

Blockchain technology can be deployed to create a marketplace for electric power supply. Microgeneration of electricity through home power generation using solar energy supplements traditional power supply and promotes the use of renewable energy sources. Using smart meters, a record of produced and consumed electricity for each user in the grid can be maintained on a blockchain with credits/currency allocated to the user for surplus power supply and credits redeemed for power consumption. This essentially creates a transparent, hassle-free and efficient energy market.

**3.9 Finance**

Cryptocurrency was the first blockchain application. Bitcoin gave the individual full possession over her money in the digital realm by making her the owner of a cryptographic key necessary for the transfer of funds. But the transfer between individuals is only the most basic program you can perform on a unit of value. More complex transaction types can be built into a cryptocurrency that replicate the full suite of financial instruments, such as loans, bonds and stocks, now offered by most institutions. Blockchains may also increase efficiencies behind the scenes at financial institutions especially in the process of interbank settlement.

For example, the Depository Trust and Clearing Corporation in New York City, a company that operates as a third party in the business of securities trading, has plans to begin recording $11 trillion worth of credit default swaps in late 2018. Others in the blockchain space are hoping to use the technology to ensure that access to basic financial tools are equally distributed. To this end, companies are leveraging cryptocurrencies to provide low cost remittance services for immigrant populations, and microloans and banking services for businesses and individuals in underdeveloped nations.

**3.10 Identity**

Bitcoin gave individuals control over when and how they spend their money. Blockchain technology may give individuals the same control over their reputation and credentials by decentralizing the process of authentication and authorization. Today most internet services offer users one of two ways to authenticate their identities. They either require users to create a unique registration for that individual site; or, they outsource this identity verification to another larger web service such as Google, Facebook, or Twitter. Blockchain applications have been proposed that allow users to manage accounts containing various authenticated fragments of their identity, which they then can selectively disclose. Blockchain-based identity management solutions have been proposed as a way to provide emergency processing of refugees who were forced to leave their countries of origin without documentation. And in the future, people who use blockchain identity management systems, may be able to more easily recover their records in the case of emergencies.

**3.11 Supply Chains**

Blockchains have been proposed as a replacement for documentation processes in the shipping industry, due to the many geographical regions and jurisdictions that a product moves through on its way to the consumer. One break in the chain of documentation can result in delayed shipment and lost profits. Blockchains may provide a way for all certification and documentation to be gathered in one place that is accessible to all parties but impossible to falsify. As products move between ports, blockchains may also provide documentation to the consumer about the lifecycle of a product, information that may ethically inform their choices about what to buy. Blockchains may also aid in securing the pharmaceutical supply chain to reduce the prevalence of counterfeit drugs.

**3.12 Internet of Things and Edge Computing**

The Internet of Things is not a one-way street. It is transforming everyday appliances into Internet portals, while also using those devices to harvest data. For example, cameras in our cars monitor surrounding vehicles and alert drivers when they’re getting too close. Edge computing is a strategy for moving the computations running the Internet of Things onto the devices that are themselves providing data feeds for the system. Blockchains may also provide a way to authenticate users across multiple IoT devices and to secure sessions. In scenarios where the price of IoT services is determined by rate of usage, blockchains and smart contracts may offer a way to transparently meter service delivery. In all pricing schemes, blockchains may provide a new way to settle debts quickly and securely.

**Chapter 4**

**Challenges**

Companies and developers are working to broaden the functionality of blockchain technologies. The prevailing ethos of the community is that no idea is too big. The infrastructure these ideas are built upon, however—the blockchain designs themselves—are not yet able to support the complexities that their inventors have in mind. Important technical developments are still outstanding, regarding the usability and security of blockchain technology. In addition, there is considerable uncertainty as to how specific applications of blockchain technology will fit into current regulatory schemes.

**4.1 Scaling**

One undeniable aim of the typical blockchain or cryptocurrency developer is to design a system that will attract as many users as possible. This is perhaps true of any startup. But it is particularly true of blockchain-based startups, which are implementing applications on top of a novel cryptocurrency. In these cases, the demand for the service directly impacts the price of the currency used to operate the application. While mass adoption at first seems desirable, no blockchain now available to the public is ready to support any amount of heavy traffic. This fact is aptly demonstrated by the constraints of the two most popular blockchains. Bitcoin is able to process around seven transactions per second. Ethereum, while faster, can still only handle around 20 transactions per second. Both rates pale in comparison to the performance of transaction networks such as Visa and Mastercard which process thousands of card swipes per second. Computing applications will require processing capabilities nanosecond to femtosecond (ns—fs) range. Most of the applications that are being proposed by blockchain startups will require a high capacity for data storage. For example, an application that uses a blockchain to execute insurance contracts and automatically dispense reimbursements for claims will require access to data about the customer profile as well as any other documentation that is relevant to the case. Given the state of the technology, it is not feasible for all this data to be stored on a blockchain. Distributed file storage systems may provide a solution, but they are still under construction [5].

**4.2 Security and Reliability**

Although the design and code for most blockchains are publicly available, their updates and releases are not formally verified or validated for security and reliability. Such practices have led to coding errors, vulnerabilities, and bugs that have caused substantial financial loss to users. Blockchains are fast becoming a repository for applications known as “smart contracts.” Smart contracts are transactions that are programmed to follow complex rules, which, in the setting of a blockchain, are then automatically and irreversibly executed. For example, a blockchain could be used to make a transaction that would execute only if the Pittsburgh Steelers were demonstrated to have won the Super Bowl in 2018. Writing smart contracts is a new skill that is fraught with peril. Once written, these programs are irreversible. Developers must be sure that the code they write does what they think it does. Developers must also understand the business logic of their programs, to ensure that they function exactly as intended.

**4.3 Accessibility**

Blockchain-based applications require users to learn an entirely different set of security measures than the ones to which they are accustomed. Rather than logging into an account controlled by a third party, blockchain applications grant their users direct access to any information they have stored on a blockchain. It is the responsibility of the user to secure the cryptographic keys that grant them this access. Or, should users choose to entrust a third-party with their cryptographic keys, it is their responsibility to vet those services. This new paradigm will require an educational campaign. To date, those efforts have been insufficient. Nearly nine years have passed since the Bitcoin project was initiated. Yet, it is still commonplace for individual wallets to be hacked and for third-party services to announce lost funds. One potential method for encouraging good security practices is the development of a Blockchain Input/Output certificate of authenticity and compliance. This certificate would provide a set of definitions and procedures that could help to standardize the input and output interfaces of blockchains. This would not only help to standardize application interfaces for blockchains, but also provide a way to standardize interoperability between individual blockchains.

**4.4 Regulation**

The same features of a blockchain that make them desirable have also placed them in a legal grey area. It will be necessary to cultivate open and steady communication between regulators and blockchain developers. Both sides face a steep learning curve about how the technology works and what regulations may pertain to its deployment. In some cases, compliance can be ensured through proper implementation. In other cases, the issues may be best resolved by fundamentally adapting the underlying technology. The following are some of the problem areas that the IEEE has identified.

• Right to be forgotten – Blockchains are marketed as indelible, timestamped records of digital events. The term used by developers is “immutability.” If a blockchain is immutable, then any new piece of information added will remain there for the lifespan of the technology. In such a system, it is unclear how applications will be built to comply with laws that protect the user’s right to be forgotten, such as the General Data Protection Ruled passed by the European Union in 2016.

• Custody of data – Data added to a blockchain is replicated on every participating computer. And if the system is entirely open, then every record is also accessible to anyone who cares to download it. Without restrictions, it is neither possible to control nor to detect the physical location of data on the blockchain. It is, therefore, impossible to assign it to a single jurisdiction.

• Privacy – Blockchains are fully transparent. While the transaction and data flowing across them is attributable only to pseudonyms, this level of obfuscation is not enough to guarantee sustained anonymity to users. It should be assumed that without enhancements the identity of all accounts on a blockchain will eventually be exposed through network analysis. Without a higher level of privacy guarantees, blockchains will be incapable of complying with consumer protection laws such as the Health Insurance Portability and Accountability Act (HIPAA) [4].

**Chapter 5**

**Conclusion**

In a plethora of blockchain based applications and experiments, faith on the longevity of blockchain technology, is increasing. Scalability and consensus algorithms are areas of growing research in order to make blockchain more adaptable for businesses of larger scale. Areas like taxation, education, insurance are yet to see a major overhaul via blockchain adoption and these can be the focus areas of future research in blockchain. Acceptance of cryptocurrency by governments and establishment of regulations governing them are very important to ensure ethical use of cryptocurrency. The public blockchains also provide an opportunity of mining interesting patterns of cryptocurrency usage, user behaviors and monetary networks across the globe.

There’s no doubt that blockchain is a hot issue in recent years, although it has some topics we need to notice, some problems have already been improved along with new technique’s developing on application side, getting more and more mature and stable. The government must make corresponding laws for this technology, and enterprise should ready for embrace blockchain technologies, preventing it brings too much impact to current system. When we enjoy in the advantage of blockchain technologies bring to us, in the same time, we still have to stay cautious on its influence and security issues that it could be have.

**Chapter 6**

**References**

1. Journal article - Supriya Thakur Aras. “Blockchain and Its Applications – A Detailed Survey”, International Journal of Computer Applications (0975 – 8887), Volume 180, No.3, December 2017
2. Journal article - Iuon-Chang Lin. “A Survey of Blockchain Security Issues and Challenges”, International Journal of Network Security, Vol.19, No.5, PP.653-659, Sept. 2017
3. Journal article - Zibin Zheng. “Blockchain Challenges and Opportunities: A Survey”, International Journal of Web and Grid Services, December 2017
4. White Paper – Morgen Peck, “Reinforcing the links of blockchain”, IEEE Future Directions Blockchain Initiative White Paper, November 2017
5. Study – “Blockchain: The next innovation to make our cities smarter”, Federation of Indian Chambers of Commerce and Industry, January 16, 2018
6. Study – Nikolas Roby. “Application of Blockchain technology in online voting”, University of Maryland University College, 2017
7. Journal Article – Ahmed Ben Ayed. “A Conceptual Secure Blockchain based electronic voting system”, International Journal of Network Security & Its Applications (IJNSA) Vol.9, No.3, May 2017
8. Study – Yi Liu and Qi Wang . “An E-voting Protocol Based on Blockchain”, Southern University of Science and Technology, Shenzhen, China
9. Study – Ivo Kubjas. “Using blockchain for enabling internet voting”, January 6, 2017
10. Article – Phillip Bouche. “What if blockchain revolutionized voting”, European Parliamentary Research Service, Scientific Foresight Unit (STOA), September 2016-PE 581.918
11. Study - Binaifer Karanjia. “Blockchain in public sector”, Federation of Indian Chambers of Commerce and Industry, January 2018