# Blockchain Technology

1. Draksharam Ravi Teja, 2. J. Siva Lakshmi 3. Ch.Supraja 4. Ch. V. Subramanyam
Dept. of Electronics and communication, NRIIT, Guntur, A.P

5. Dr.M.Rakesh,
Associate Professor
Dept. of ECE, NRIIT, Guntur, A.P

***Abstract***

*Blockchain, in simple words can be defined as a distributed and decentralized database that stores each exchange of information or any kind of digital event that occurs between the participants in the form of block that are linked to each other, Each Block or the Digital event is verified by the consensus of all other participants in the system based on majority which is why it's otherwise called as Digital Public Ledger. As an individual and separate block is created for each new digital event without any change of previous events, the data once entered into blockchain is indestructible and can be traced back to any previous event possible.*

*It helps to form a democratic distribution and handling of data and can effectively eradicate the requirement of middlemen in present day scenario, on whom most of our daily life rely on. The major example of its work can be Bitcoin, a peer-to-peer digital cryptocurrency which have the potential to eliminate the need of financial institutions like Banks to transact the money from one person to another.*

*In this paper, we discuss about the Blockchain technology and its wide range of applications in various fields both financial and non-financial offering the decentralized and trustful solutions to many issues we face today and its potential to shape the harmonious democratic and decentralized society which was lost in the smokes of monarchy and middlemen system. Also how blockchain be a dominating technology for coming 20 years like what internet is for last 20 years*

***Keywords—***
***decentralized;trustful;democratic;dominating;blockchain***

## I. INTRODUCTION

Blockchain, in simple words can be defined as a distributed and decentralized database that stores each exchange of information or any kind of digital event that occurs between the participants in the form of block that are linked to each other, Each Block or the Digital event is verified by the consensus of all other participants in the system based on majority, which is why it's otherwise called as Digital Public Ledger. As an individual and separate block is created for each new digital event without any change of previous events, the data once entered into blockchain is indestructible and can be traced back to any previous event is possible. Also each block being encrypted by a highest level cryptography provides an immense security for the data stored in the blockchain

Tough most people today know it as the backend technology of the famous cryptocurrency Bitcoin, But Blockchain technology isn't which confines to the financial sector it holds vast promise for every business and every sector possible

## II. WHY BLOCKCHAIN?

Blockchain promises an astounding future and can also be stated as the next generation of internet. This resolves many issues and problems that internet unable to handle and get a proper solutions. We'll see past how blockchain be better replacement of Internet

### *A. Internet of Information*

From past few decades we have the Internet of Information which means we exchange the information from one another i.e. if an Image is shared over the internet only copy of it is transferred to the other party not the original one so being stated as a democratic information.

### *B. Requirement of Middlemen System*

These works well for exchange of information but when it comes to exchange of assets or value sending a copy is not a good practice because one should not possess the money that he transferred to another person and this is applicable to all kinds of assets like Vote, Music, Art, Intellectual property ,Stocks, etc. This problem which otherwise stated as the Double-spending problem by Cryptographers.

Due to this problem we mostly rely on the big intermediaries otherwise, called as Middlemen further in this paper, who perform all the transactions, verify and authenticate people and their actions for all the value related matters. These creates a centralized system which opens up a way for numerous problems and mischiefs like it can be hacked or tampered easily, Also exclude the people from the system, As people who don't have enough money to have a bank account there by excluding them from participating in economy

### *C. Internet of Value*

Unlike Internet of Information, This Internet of value is a vast, global distributed ledger where different kind of assets can be stored, moved, transacted, exchanged and managed .i.e. running on the millions of computers all around the world

without any requirement of any Middlemen. Also providing the native medium for the value. Blockchain perfectly works as the Internet of value.

## III. BACKGROUND

The footprints of the blockchain technology can be traced back to 1991 where Mr. Haber and Mr. Stronetta worked on a system that works in such a way that it digital timestamps the documents so that they cannot be tampered easily, they implemented Merkle Tree Mechanism which improves the efficiency of the Block, These is very similar to blockchain technology what existed today.

The Blockchain technology as we know it today is first conceptualized by anonymous person (or a Group of persons) known as Satoshi Nakamoto in the paper he published in 2008, where he explains the concepts of perfect working blockchain with all the different concepts linked to like Proof-of-work, mining, etc. which we'll discuss further in the paper, Later he used to develop the World's first decentralized cryptocurrency Bitcoin at following year which creates boom into the World of Economy

After a Bitcoin success a 19-year old programmer Vitalik Buterin created a another blockchain known as Ethereuem with its own cryptocurrency Ether, It takes Blockchain to another level with an introduction of Smart contracts, a self-executing code very similar to contracts we make in the physical world which opens-up the blockchain technology to be used in wide range of sectors

## IV. WORKING OF BLOCKCHIAN

Blockchain as the name suggests is a blocks of data, which are linked to each other in chronological fashion like a chain, each block contains 3 things,

- Data
- Hash of the block
- Hash of previous block

The Data that is stored in the block total depends on the type of the blockchain that block existed, as bitcoin blockchain contains the data in block which includes the information of the sender, receiver and amount transferred between them.

Hash is the unique identification cryptographically provided to the block can be defined as the digital fingerprint for our better understanding, it is used to identify the block in the blockchain and all the contents in it, any change in the block causes the block to change its hash code so any change in data of the block, it can't be the same block it was previously securing the tampering of the information

The third and most important thing the Hash of previous block is what makes the Blockchain, a Chain of blocks, it links this block to its previous block making a chronological chain of blocks, As we discussed earlier any change in the data in block changes it's Hash value making that block all the blocks following that in blockchain invalid causing a failure, this mechanism offers an immense security for the Data making it tamper-proof and secured.
The first block in the chain which doesn't contain any previous block doesn't include the Hash of previous block called as Genesis Block.

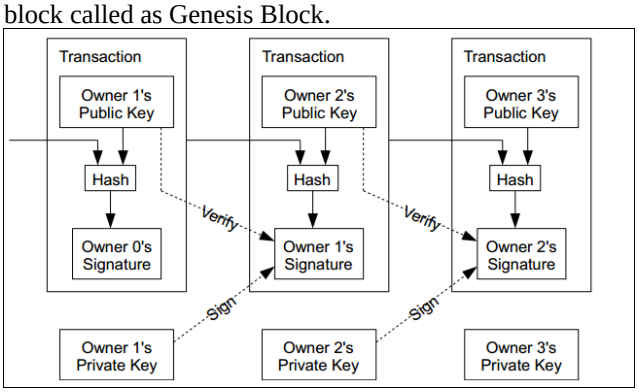



***Fig: Hash mechanism in the blockchain***

When a new series of digital event occurs in the blockchain, a block is created for every period of time, known as Block time, That block contains all the details of the transactions happened during the Block time. And these Trivia doesn't end here, there a hectic tough secured process to add this block to the blockchain,

- The Cryptographic Puzzle must be solved in order to create a valid block.
- This Puzzle's solution shared along all others nodes in the blockchain network. These above two steps collectively called as Proof-of-work
- Further this proof-of-work is then verified by all other node there by approving the block to be added in the blockchain, if only if the submitted Proof-of-work is found to be genuine by majority of nodes in the network

This verification of blocks through proof-of-work mechanism offers the intense security levels which makes the blockchain un-hackable

Tough as we discussed earlier, Hashes offer the security but today we've computing power that calculate the hashes in a snap. There by dissolving the blockchain security.

Further, with the Ethereuem blockchain a new word creeped into the Blockchain World called Smart contracts, these are nothing but a small piece of computer code which acts as a contract for particular things to happen in the blockchain directly peer-to-peer,

## V.PROOF OF WORK

In Block Chain technology, before a block to be added to the chain, a cryptographic puzzle must be solved by a computer and that computer must share the obtained solution to all the other computers on the network. This process is called Proof of work.

Consider a case say, three nodes solved the cryptographic puzzle for a same block, then arises a question that whom block should we consider here a rule named Longest Chain rule comes into scenario, These 3 nodes will have different computational power so different time it'll take for each of them to get the solution, as other miners will also get there blocks done, they'll add their blocks to the one of the block of that 3 miners, which submitted the proof-of-work first, i.e., who have the high computational power, so out of the 3 blocks, the block having the longest chain is added to the blockchain and been rewarded for his/her work.

A block is added to the chain only if the network verifies the Proof of work. This verification of block through proof of work to decide whether it should be added to the Block Chain or not is called Mining. Mining is an innovation that makes decentralized record-keeping possible.

In the process of Mining, miners are isolated tons of resources, first they are buying expensive hardware called ASIC (Application Specific Integrated Circuits) and then they need electricity that burns off computers at high temperature, which leads to the destruction of computers. So, in-order to overcome the heating issue of computers, in some cases fans are installed to cool down the hardware. But all of that energy is used to solve the block and after that block is solved that block gets added to the public blockchain. All these resources are used to solve the block well first itself and to accurate each transaction.

### *A. Proof-of-work of Bitcoin*

Large cryptographic networks like bitcoin uses the Proof-of-work algorithm as its foundation because it provides complete decentralization of power and control over the distribution and implementation of major technical and economic changes in the network.

In Bitcoin mining, miners require hundreds and thousands of computers mining for Bitcoin. They are all trying to solve these blocks using vast computing power. Bitcoin blocks are created every 10 minutes on an average.

To attack bitcoin, the proof of system requires the hacker to own at least 51% of the network's hash rate or computing power, which is virtually impossible considering the size of the bitcoin network and it is of considerably high hash rate.

However, small proof of work-based networks are easier to hack because attackers can gain 51% of their computing power at very low cost.

For instance, the Ethereuem network is based on a Proof-of-work system. Ethereuem blocks are created every 17 seconds on an average. When Ethereuem network split into two independent networks – Ethereuem Classic (the original chain) and the hard-forked Ethereum –former Ethereum supporters including Chandler Guo threatened to use the 51% attack against Ethereum Classic. Since, it was affordable to gain more than half of the network's total computing power given the small size of the Ethereum Classic network at the given time.

### *B. Transaction fees:*

Transaction fees are included with your bitcoin transaction in order to have your transaction processed by a miner and confirmed by the Bitcoin network. The space available for transactions in a block is currently artificially limited to 1 MB in the Bitcoin network. This means that to get your transaction processed quickly you will have to outbid other users.

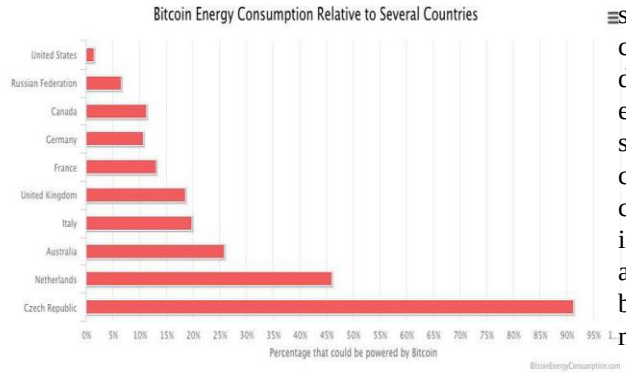
[The satoshi is currently the smallest unit of the bitcoin currency recorded on the block chain. It is a one hundred millionth of a single bitcoin (0.00000001 BTC)]

- These are the estimated fees you should use depending on how fast you would like to obtain the first confirmation for a typical transaction.
- When making a Bitcoin transaction, recipients usually require somewhere between 2 and 6 confirmations to consider the transaction as valid.
- The transaction fee you pay will only affect the time you have to wait until the first confirmation.
- Once your transaction is included in a Bitcoin block and thus obtains the first confirmation, you will need to wait approximately 10 minutes for each additional confirmation.
- After the first confirmation, the waiting time for each additional confirmation is completely independent of the transaction fee you paid.
- Because of the decentralized nature of the Bitcoin network and the fact that there is sometimes congestion in the available block space (because of the 1MB limit).

If we consider Ethereuem mining, miners play an important role in making sure Ethereuem works. Many new users think that the sole purpose of mining is to generate ethers in a way that doesn't require a central issuer. Ethereuem's tokens are created through the process of mining at a rate of 5 ether per mined block.

### C. *Energy Consumption:*

Proof of work is data that is costly and time-consuming to produce but easy for others to verify. The Bitcoin POW mechanism is so costly that it consumes the same amount of electricity it takes to power a country like Switzerland in one year. Bitcoin's current estimated annual electricity consumption is 61.4 TWh, which is also equivalent to 1.5% of the electricity consumed in the USA.




## V. SMART CONTRACTS

Smart contract are self-executing contracts with the terms of the agreement between buyer and seller being directly written into lines of code. The code and the agreements contained therein exist across a distributed, decentralized block chain network. Smart contracts permit trusted transactions and agreements to be carried out among disparate, anonymous parties without the need for a central authority, legal system or external enforcement mechanism. They render transactions traceable, transparent and irreversible. While block chain technology has come to be thought of primarily as the foundation for bitcoin, it has evolved far beyond underpinning the virtual currency. A smart contract is a computer protocol intended to digitally facilitate, verify or enforce the negotiation or performance of contract.

### A. *Background*

Smart contracts were first proposed in 1994 by Nick Szabo, an American computer scientist who invented a virtual currency called "Bit gold" in 1998, fully 10 years before the invention of Bitcoin. In fact, Szabo is often rumored to be the real Satoshi Nakamoto, the anonymous inventor of bitcoin, which he has denied.

Szabo defined smart contracts as computerized transaction protocols that execute terms of a contract. He wanted to extend the functionality of electronic transaction methods, such as POS (point of sale) to the digital realm. He was referring to the sale and purchase of derivatives with complex terms. The main aim of smart contracts claim that many kinds of contractual clauses may be made partially or fully self-executing, self-enforcing, or both. The term aim of smart contracts is to provide security that is superior to traditional contract law and to reduce other transaction costs associated with contracting and also to reduce fraudulent in them.

Various crypto currencies have implemented types of smart contracts. It is mostly used more specifically in the sense of general purpose computation that takes place on a block chain or distributed ledger. In this interpretation, used for example by the Ethereuem foundation and IBM, a smart contract is not necessarily related to the classical concept of a contract, but can be any kind of computer program. Smart contract concept is rooted in basic contract law. Usually, the judicial system adjudicates contractual disputes and enforces terms, but it is also common to have another arbitration method, especially for international transactions.

### B. *Ethereum*

Ethereum implements a nearly truing-complete language on its block chain, a prominent smart contract frame work.

Ethereum is an open-source, public, block chain based distributed computing platform and operating system featuring smart contact functionality. It supports a modified version of Nakamoto consensus via transaction-based state transaction. Ether is a crypto currency whose block chain is generated by the Ethereum platform. Ether can be transferred between accounts and used to compensate participate mining nodes for computations performed. Ethereum provides a decentralized Turing-complete virtual machine, the Ethereum virtual machine, which can execute scripts using an international network of public nodes.

Ethereum was proposed in late 2013 by Vitalik Buterin, a cryptocurrency researcher and programmer. Development was funded by an online crowd sale that took place between July and august 2014. In 2016, as a result of the collapse of the DAO project, Ethereum was split into two separate blockchains, the new separate version became Ethereum, and the original continued as Ethereum Classic.

The Ethereum virtual machine is runtime environment for smart contracts in Ethereuem. It is a 256-bit register stack, designed to run the same code exactly as intended. EVM is specified in the

Ethereum Yellow Paper. It is sandboxed and also completely isolated from the network, file system or other processes of the host computer system. In February 1, 2018, there were 27,500 nodes in C++, Go, Java, Python and Web Assembly.

Ethereum can be used to codify, decentralize, secure and trade. It is developed as a platform which facilitates peer-to-peer contracts and applications via its own currency vehicle. Next generation innovators are now seeking to apply these same principles to a variety of online services they believe could be built in the decentralized format, armed with a little effort, know-how and the will to charge forward into the unknown. Although a new field, decentralized apps are growing in number and many now exist in various stages of completeness, from concept to working prototype and functional platform. These Smart contracts can be implemented in various fields at ease like documentation, copyrights, royalties, etc.

## VI. PROOF OF STAKE

Proof of work tough a secured mechanism that offers the immense security and a democratic consensus that helps blockchain stay decentralized and democratic in manner. But, let's consider a case of Bitcoin, The miners sometimes combines there computing power to complete the Proof-of-work faster and distribute the rewards equally, these are called Mining pools, As most of the miners come together say, 51% miners are together combined there computing power to generate Proof-of-Work for the further transactions of Bitcoin, Now there's risk of approval of fake transactions and make the blockchain centralized losing its sole purpose and essence. So, there is need to be a better algorithm than proof-of-work which is a Proof-of-Stake.

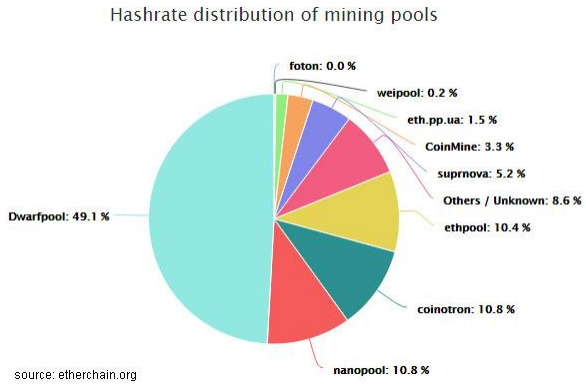



***Fig: Ether pools in the Ethereum Blockchain***

Proof of Stake is a type of algorithm by which a cryptocurrency Block Chain network aims to achieve consensus. Proof of Stake (PoS) states that a person can mine or validate next block transactions according to amount of cryptocurrency a node holds.

In Proof of Stake, miners are called as Validators and there will be block that needs to be generated. Proof of stake doesn't let people to mine new blocks. Validators do not receive a block reward, instead they collect network reward as their fees.

For Example: If there are four validators, each validator deposits their money to the Block Chain to get the opportunity to validate (sign) a block. Later, the one who has the most money takes up 38% of the block, elevator two has 25%, stake validator 3 has 21% and validator 4 have 16%. In mining, the chances you had of solving the block was dependent on the hardware that you have. But bigger your stake which bigger the chance you have of solving the block. The validator one with the largest stake (38%) wins and gets assigned the block, validator one is rewarded not with new coinage but with transaction fees. It is true for stake that it's dependent on how much you're willing to stake to solve the block.

In 2011, a bitcoin forum user called Quantum mechanics proposed this Proof of stake technique.

### *A. Proof-of-Work vs Proof-of-Stake*

Let's take a look at the facts which says Proof of Stake is better well:

- Proof of stake is actually more eco-friendly than mining in proof of work, all the hardware that you're using to compute in mine burns up a lot of energy in order to secure a Block Chain. It's estimated that both Bitcoin and Ethereum burn over 1 million dollars' worth of electricity and hardware costs per day as part of their consensus mechanism while proof of work requires miners to effectively burn computational power on useless calculations to secure the network but Proof of Stake effectively decrease the burning so no real world energy resources are wasted.
- With Proof of work new coins can be generated by solving blocks and for bitcoin, the coin supply raises up at 21 million which is supposed to have in a 100 years from now while Ethereum doesn't have a supply capability right now, they are planning to partially burn transactions fees like ether deflationary so that it becomes more valuable over time because with the proof of stake no new coins can be generated or mine.
- Proof of Stake discouraged centralized cartels, bitcoin right now has a lot of mining problems. If you go to Block Chain info, mining pools as of today you will see that the top ten mining team controls 83.1% of the bitcoin mining power and out of 10 mining pools, 8 of them are located in china

but they're way to many mining cartels that have too much power proof mistake would prevent that.

- After Krypton, a Proof-of-work network, was recently hacked, the Krypton development team announced its transfer to a Proof-of-stake system. "Krypton has decided on the following temporary course of action in order to protect KR from being stolen from exchanges through a double spend: Krypton is moving KR from an Ethereum-based proof-of-work blockchain to a Bitcoin-based proof-of-stake blockchain," announced the developers. Buterin openly supported this move by stating that they have not seen a single case of Proof-of-stake network being hacked.
- Proof of stake mistakes of 51% attack virtually impossible. First of all, what is 51% attack? Let's say there are hundred nodes in the network, 51% of bad actor must control 51% of the network to implement an attack on blockchain. So that it benefits them. However with Proof of work mining, this is done by having more raw computing power than 51% of the entire network which is a very large expense. With proof of stake, a validator would have to control at least 51% of all of the digital currency in existence which would make it very expensive.
- With Proof of Stake, Ethereuem is also implementing unbearable penalties for people who are trying to duplicate blocks they'll actually destroy your ether in your stake. Here's is a theory to make 51% attacks extremely expensive, so that even a majority of validators working together cannot rollback finalized block without undertaking an extremely large economic loss. This loss is so large that a successful attack would increase the price of the underlying cryptocurrency.
- Let us assume that the validator with a large stake A can contribute to the security of the cryptocurrency and B (possess stake less than A) will get endanger to his large stake by manipulating the blockchain by doing so he will devalue his fake or lose it all together and this all leads back to making Proof of Stake much more secure and much more stable so there you have the benefits of proof of stake now.
- Because of initial distribution problems, long range attack, bribe attack, coin age accumulation attack, free computing attacks Proof of Stake is by no means perfect but the genius over the Ethereum foundation are developing distinct POS system called Casper that's another beast because it's a mixture of Proof of work and Proof of Stake.

One and only major disadvantage of Proof of Stack is giving priority to validator who invests more on block. This makes Block Chain Technology trustless and worthless, what many experts, including Ethereum co-founder Vitalik Buterin, may regard as the greatest merit of the Proof-of-stake system can actually its main disadvantage. A system where the major stakeholder enjoys extensive control and authority over both technical and economic aspects of the network creates a major economic and technical problems

In a Proof-of-work network, the majority of voting power when implementing important changes to the system is divided among miners, developers and other crucial members of the community. Meanwhile, in a Proof-of-stake network major stakeholders have a technical ability to make any changes they like without considering the opinion of the community, businesses, miners, etc.

### *B. Proof-of-Stake Reverified*

Tough Proof-of-Stake works better the Proof-of-Work, it holds some disadvantages too. They can somewhat be eliminated with a new changes in this mechanism that's already been working better.

They are:

1. Each Validator's Stake value is to be fixed rather than giving choice to validator to invest whatever (Practically Higher) amount he wants.
2. By doing so, each validator invests the same amount there by having the same level of probability to get a chance to validate the block
3. The Validator is selected in a Random fashion rather than priority that depends on the stake he holds,
4. We can implement a code that checks that not the same validator is selected again and again within a period of time, though they're selected randomly.

These Steps can make the Proof-of-Stake somewhat better than it is now and can make more secured and decentralized and democratic blockchain.

Casper API is an data storage platform. It is required just because of increasing number of decentralized applications, we need a better platform than centralized cloud storage for storing data. Casper API provides services like data storage, backup copy storage, and content delivery network. Casper API will issue its own currency unit called CST for all transaction in this platform. Casper API has been given high rank in many reputed ICO tracking sites.

High speed access: The decentralized data storage system reduces possible delays and increases accessibility

Cost reduction: Data storage and distribution for end users costs 3 times lower than traditional CDN and cloud storage solutions.
Data protection: Each file is stored by 4 independent storage capacity providers.
Security on a corporate level: confidential transactions through a private channel using a cryptographic protocol similar to the lightning network.

Also Casper is the new project that is currently under development by the Ethereum Blockchain developers which punishes the Validators if he performs any kind of fraud in the blockchain by slashing the stake that he previously invested. It doesn't end here, the validators also get their Stake slashed if there node uptime is so high, i.e. punished for their laziness and carelessness.

## VII. FUTURE FOCUS

Blockchain technology mostly known as the technology that's behind all the cryptocurrencies due to the impact of Bitcoin on the society because of its arrival just after the financial crash in 2008. People after that just deep rooted in their thoughts that a Blockchain is just for Cryptocurrencies. Also most of the research and development had been done and even be doing in the financial sector itself as we can see most of the blockchains today have their own cryptocurrencies included in the chains tough created for other applications.

### *A. Blockchain beyond Cryptocurrencies*

Blockchain is beyond just being a crypto-technology that have immense potential to change the phase of world towards a better society. It's is estimated that Blockchain will create such an impact on the world in similar fashion as Internet have influenced our lives from past 20 years. Blockchain can implemented in all kind of sectors possible with infinite possibilities.

For the sake of explanation, we'll take Internet as the example and further see how Blockchain can be Internet 2.0

When Internet is first introduced in to the world, it's just a mere application to connect people into a single network to exchange information all around the world in a snap! Later it evolved beyond imaginations as now being a platform for E-commerce, IOT applications and prime centric for advertisements, Stake holding, Banking, Social media, Social relationships and anything existed. It's been into everything that experts are expecting that there won't be any sector left without Internet.

Tough it take over the world like charm, it lacks the two most important factors that it had to have for sure.

They are:

- Trust
- Elimination of Middlemen

Internet must establish trust between people without any third parties, It estimated to eliminate the Middlemen instead created the real big ones like Facebook, Google, Microsoft to name a few. Even the money transactions are centralized with the payment systems like PayPal.

As we already know, the main essence of the blockchain is Trust and Elimination of middlemen there by connecting people peer-to-peer establishing trust without any middlemen to spy upon as we see in recent cases. With the smart contracts and trustworthy proof-of-work mechanism it can implemented at all kind of sectors which includes the both with exchange of information and exchange of value.
For Explanation, let us take the Music industry, where the creators have to be involved with the intermediaries like Spotify to make money of their content, as we all know recently Artists' files a fraud on Spotify about their Royalty issues,

In the above scenario just imagine the implementation of blockchain and a smart contracts where Artists directly be in contact with their listeners and subscription amount will be transferred to them immediately and directly with the smart contracts. Also the copyrights and royalties can also be issued in the similar fashion, here there is no involvement of an intermediaries to establish trust between the Creators and the Customers, and one such project is Mycelia, a node-to-node music platform.

Blockchain can be implemented in many industries to eliminate the need of intermediaries to establish Trust between people. Different kinds of Blockchains can be created for different kind of purposes.

- Private Blockchains to use within the organization or group of people privately to exchange information between them, they can be like Military, Defense, Secret Organizations, etc.
- Public Blockchains to use publicly while information in them is accessed by all the public, who have the authority to view, add the new blocks
- Hybrid Blockchain is the combination of the Public and Private Blockchains where some parts of data is visible to public while some will be private and Right to create the new block can be restricted too to avoid any kind of issues

These three types of blockchain can be implemented where ever they are required like Hybrid Blockchain can be implemented by the government where some data can be public while some other data needs to remain private. The best example for this scenario is the implementation of blockchain to keep records of Land entitlements, it helps in elimination of the fraud

and tampering of data and to create any kind of fake documentation, which eliminates the need of a lawyer and a long judicial system, to verify the documentation saving both time and money to solve any kind of issue that's aroused. Here if anyone want to know the measurements of a land they can see them without revealing the information of the Owner of that land. This can be achieved by implementation of the Hybrid blockchain and smart contracts included.

Blockchain can also show us the better solutions for our social problems one such project is that creation of blockchain where the Politicians i.e., Public representatives to be answerable to the general public

### *B. India and Blockchain*

India is a developing country. It is the world's sixth largest economy by nominal GDP and the third-largest by purchasing power parity. India has one of the fastest growing service sectors in the world. India has become a major exporter of IT services, BPO services and software services with $154 billion revenue in 2017. Utilization of technology results in saving labor. Technology offers new opportunities and the discovery of new ideas. India's first ever indigenous supercomputer was a major milestone in modern India's technology journey. The southern part of India is responsible for the majority of technology and advancement the country has made.

The golden triangle of IT and technology forms the backbone of Indian manufacturing, R&D, science and technology. Privacy of the data is the most important consideration; there are ways to secure data by not even connecting to a network. But if existing IT infrastructure featuring accounts and login is not sufficient for the security of digital identity, then the problem might be solved by block chain technology. It offers new tools for authentication and authorization in the digital world that preclude the need for many centralized administrators. By formalizing and securing new digital relationships, the block chain revolution is posed to create the backbone of a layer of the internet for transactions and interactions of value.

The fundamental attributes of block chain is consensus, trust, immutability, Provence and smart contracts. Privacy key cryptography enables push transactions, which don't require centralized system and the elaborate accounts used to establish digital relationships. As we discussed earlier block chain can be implemented in many areas. Health care is one sector that block chain technology has transformed to the core. Making it more transparent, accessible and secure. A country like India, where access to adequate healthcare is a privilege generated to few, and block chain could ensure that health care services reach the grassroots and is affordable to all.

Block chain can be implemented in many sectors like healthcare, agriculture, Insurance, financial, media and entertainment sectors which are facing many problems. Take agriculture, for example. With 119 million farmers, 16% of the Indian country's gross domestic product and close to 8,000 farmer suicides a year, framing is in distress. The farmer's long march in Maharashtra recently. The reasons for the crisis are well known—ineffective subsidy management, lack of insurance and loans, small land holding, lack of mechanization and lack of information. The block chain is the best suited to solve such problems. Tractor and frame equipment sharing, through an uber-like model, can be powered by the block chain. You can take it one step further and have fractional ownership of tractors, with multiple-party financing, to solve the mechanization problem. Farm subsidies can be much more effectively managed through block chain-based mechanisms. The other big transformational problem in India is energy, especially in rural areas. One of the big reasons for lack of electrification is the current centralized model of electricity—one central power plant, with wide distribution. For rural areas, electricity needs to be generated where it is required, and largely through clean sources like solar, wind and biogas. Through smart micro grids, powered by block chain and internet of things, power from a surplus house can automatically be moved to a deficit house, and a smart contract can settle the payments.

One of my favorite transformational use cases, in fact, is to have chit funds on a decentralized ledger, eliminating chit fund fraud and creating a parallel, decentralized banking system. This has the potential to bank the unbanked and eliminated bank fraud at the same time. The possibilities are limitless. Estonia is putting everything on a block chain, creating a country as a service;

India is the most under vaccinated country on earth, in spite of huge subsides, primarily because it is difficult to trace who got vaccinated, and where the subsidy went. Block chain can be used to address this too. The distributed ledger aspect of block chain technology is appealing to Indian companies is in contracts. When you instant a smart contracts, it is present on every node of block chain. For example there are eight nodes on the block chain, you can say that five of the eight nodes need to confirm a transaction before it is authorized. So, a change to the information can happen only when this is possible.

The smart contracts can be used for information which forms the basis of KYC documentation, ensuring that details like name, address and date of birth cannot be modified once they have been entered into the system. Reserve bank of India has been closely monitoring development related to block chain. In July 2016, Institute of Development and Research in banking technology the technology research and arm of RBI took the initiative of exploring the applicability of block chain to Indian banking and financial industry by conducting a workshop involving all the stack holders such as the

academicians, bankers, regulators and technology pointers. The participants of workshop come together to bring a white paper detailing the technology highlights several advantages of block chain technology, such as cost saving, efficiency and transparency have been highlighted.

For *Ganesh Chaturthi* festival in India, the police department has to give permission for the Ganesh pandals across the state. The police department in Visakhapatnam deployed a block chain based single window system, developed by a city based startup Zebi Data India for the purpose of clearances to Ganesh pandals. Once the online request for the pandals were registered on the Zebi block chain, the police coordinated internally with other departments such as electricity, fire, municipal departments and the civic body to assess the application. Zebi data India has earlier helped the AP police department in integrated hotel guest data by using block chain and artificial intelligence. Over 200 hotels in Visakhapatnam are connected to Zebi has also integrated land records of Amaravati, an upcoming capital of Andhra Pradesh with Zebi artificial intelligence chain.

## VIII. CONCLUSION

Blockchain has a potential to change the course of history of technological industry for upcoming years again redirecting the Humans towards their long lost culture of the decentralized society where every one trust each other peer-to-peer without a need of intermediaries, without a need of the transferring the Authority into the hands of few

Blockchain can be implemented into almost every industry we know existed, can also be used to solve our social issues in practical, decentralized and democratic manner, a step towards a utopian society. If required research and development is put into the development of this technology it'll become the next big thing after the internet.

## IX. REFERENCES

[1] "Blockchain: Blue print for a new economy", by Melanie Swan.
[2] "Ethereuem: Blockchains, Digital Assets, Smart Contracts, Decentralized Autonomous Organization ", by Henning Diedrich
[3] Blockchain revolution: How technology behind bitcoin is—Alex Tapscott & Don Tapscott.
[4] Blockchain Basics: A Non-Technical Introduction in 25 Steps—by Daniel Drescher – "Why Blockchain is needed"
[5] Bitcoin: A per-to-peer Electronic Cash System – Satoshi Nakamoto, www.bitcoin.org, doi: 2008.
[6] A Short Introduction to the World of Cryptocurrencies – Aleksander Beerentsen and Fabian Schar, https://doi.org/1020955/r.2018.1-16.
[7] How blockchain technology could change our lives – http://www.ep.europa.eu/stoa/, 2007.
[8] Global Blockchain benchmarking study—by Dr. Garrick HIlemen & Michel Rauchs, http://www.ey.com, 2017.
[9] The Blockchain – http://www2.delottie.com, 2017.
[10] Applications of blockchain technology – to banking and financial sector in India, -- IDRBT—2017.