

Limitations of Blockchain Technology with its Applications.

Ammbika V. M, DS Rao.

Abstract: Block chain is also called as chain of blocks i.e. it is collection of technologies or collection of Technologies or a bit like a block chain sack of Logo From the sack y can collect different bricks and arrange them some particular way/different way to create a chain blocks .It is decentralized i.e. no any central control or authority assigned to it .It is simple. Easy to understand and work the system. New blocks are added at the end of the block chain .It uses data structure-link list-also called as linear data structure, stored at contiguous location in work on concept of pointers. They form a chain in continuous way using array ,doubly link list-pointers are used for fast and speedy execution ,it traverse in forward direction –move ahead, backward direction-move back, operations like addition & deletion of node can be efficiently done

In this paper the small basics of Blok chain engineering i.e. permission accesses, properties with its few drawbacks are studied. Some projects of Blok chain Engineering were referred with its some good and bad features during the working phase.

This paper aim is to find drawbacks related to the Block chain combination and working in the various fields of smart city.

Index Terms: Timestamp, private block chain ,public Blockchain, Trust, Immutable, Throughput, Latency, size of blockchain, Transparency, Hash Technique, Big" O" notation.

I. INTRODUCTION

Block chain Engineering acquire different achievement .Therefore this Engineering has some limitations which merge to high cost, Government issues, working process of the Technology[1],[3].Recent Blockchain is solvent for many issues related to taxation ,financial,2.0 spend problem-without involvement if third party[1],[3].Blockchain Engineering provides solutions for such issues[1],[3].The Blockchain invent blocks considering variety of data.Related to Blockchains safeguard and certainty ,”Proof-of-work”,can be useful.Creation and Deletion of recent/new block connection is nearly not at all possible[1],[3].Blocks to hack high processing electricity is needed. Blockchain depends upon confidentiality, integrity and availability of data [2].

The hash value for new block is finned using miners [1],[3]. Depending upon “Proof-of-work”, access permissions like Read only, Write only or both are provided for block.

Revised Version Manuscript Received on 16 September, 2019

Ammbika V M , Doctorial Research Scholar in Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation,Vaddeswaram 522502,Guntur,Andhra Pradesh,India .

DS Rao,,Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation,Vaddeswaram 522502,Guntur,Andhra Pradesh,India .

In this paper is written about Blockchain Engineering basics, functions. The major limitations of the Blockchain Engineering are trust, throughput, variable size,Bandwidth,Fork,security,The working organizations of Government agencies and its very high rate.



Fig 1: Functions of Block chain.

II. HASHING TECHNIQUE IN BLOCKCHAIN TECHNOLOGY

The hash table is simple backed by an array of pointers.Instead of it containing values,,each item is simply the head pointer to the 1 st item in the list[3].So calculating the hash given you an index into the array which in turn gives you the head of the LL(i.e the first item in each list)Each List is a normal LL,which each node being a record containing the key(& other values if such exists) as well as a next pointer to the followin item in that list[3].

III. PRIVATE BLOCKCAHIN TECHNOLOGY AND PUBLIC BLOACKCHAIN TECHNOLOGY

Depending on way of access control blockchain can be called as permissionless/presence-it is open for the people, by the people and of the people and permissioned/absence block chain –maintain a record of “proof of work” i.e. flat database files[4].

IV. PERMISSIONLESS BLOCKCHAIN ACCESS CONTROL

Write only data: anyone can write data without any granted authority permission [1].

Read only data: anyone can write data without any granted authority permission. Read only permission when adding a new block or maintain a full copy of the entire blockchain, such blockchain which allow equal & open rights to all participants.since bitcoin is designed as “anyone –can –write” block chains, where block chain adders can add blocks to chains without needing any authorized permission [1]

Limitations of Blockchain Technology with its Applications

.so this increases the cost & complexity of running this block chain[4].

V. PERMISSIONED BLOCKCHAIN ACCESS CONTROL

In this mythology, identity of participants is known & authenticated. They maintain record of “Proof-of-work” [4]. In short access control layer allows certain triggers to be implemented only by specific –unique participants [4]. It is way entrepreneurs decide to work the technology either private/public block chain technology [4].

VI. PARTIAL PRIVACY

All changes done on the Block chain can be traced back to a participant /user [5].

VII. IMPOSSIBLE TO SCALE

Processing power to function (mainstream payment system) is very high.

VIII. REGULATORY NONCONTAGIOUS

EU authorities are only exploring the regulatory impact of Blockchain application to virtual currencies.

IX. ADAPTATION OF EXISTING INFRASTRUCTURE

Participant get used to a more peer- to- peer network (decentralized network) [2].

X. VALIDATION TRANSACTION

A transaction is said to be valid with respect to particular blockchain state if it is well formed & if the output it attempts to spend exist in the state, and if condition is satisfied in those output [7]. The transaction may or may not be valid with respect to a different block chain state [7].

XI. TIMESTAMP

It is the process of securely keeping track of the newly created document and modification time of a document. it assigns a time for each transaction on the block. Data of timestamp is recorded called tamper proof. Timestamp is used instead of Real Time. Blocks in Blockchain check them against real time & will try to ignore blocks that are outside of a certain range of times based on its own interval clock time.

Timestamp is calculated: $\text{Difference in } _ \text{ blocks} = \text{round}(\frac{\text{end_block_mediantime} - \text{given timestamp}}{600\text{sec}})$
 $\text{Desired_block_end_block_height} + 1 = \text{difference_in_blocks}$

XII. TRUST

Blockchain technology follow the mining protocol which helps in execution of blockchain technology [7]. The new Architecture of Trust (Levin Wear Bach-book which shows how a technology depended on foundations of mutual mistrust can become trustworthy) Different types of trust architecture are

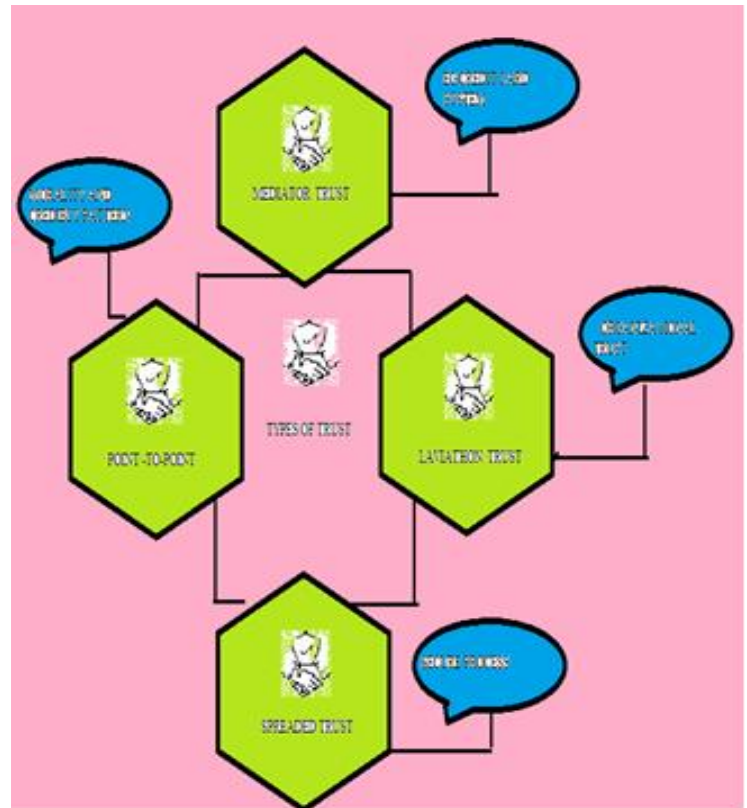


Fig 2: Trust showing Block chain Technology

XIII. THROUGHPUT

This is one of the important factor of Bitcoin –Network. it is mostly does 6-8tps transactions per sec [7]. Different processing transaction also process on Network like VISA (Visitors International Stay Admission) and Twitter (4000-5000) tps, Facebook (FB)(1000-2000)tps[7].

Frequency depends upon throughput of Blockchain Network i.e. Frequency of Blockchain Network is directly proportional to throughput i.e. they work at same level i.e. throughput of Blockchain Network can be increased by increasing Frequency [7].

Formulae: Frequency (block chain Network) “inversely proportional” Throughput (Blockchain Network) [7].

XIV. VARIABLE SIZE

Block size increase as the new blocks join the chain. Capacities of nodes vary in Block chain [8]. The two main factors considered are:

A: Small log: Nodes are not capable of processing complete copy of the Blockchain, which does not follow immutability and transparency of the Block chain [8].

B: Centralized Technology: The size of the Block is variable in Bitcoin Network [7]. It can vary from MB-GB [7]. It all depends upon the throughput of Bitcoin Network [7]. Throughput of Bitcoin in Blockchain Network is inversely proportional to size of Block i.e. it raises the levels of FB, Twitter, VISA

,(Terabytes-Petabytes).Blockchain can grow from (200 TB-300PB)[7].The Satoshi Nakamoto assumed that size of 1.0 block can be one-two MB & it can take time of 8-10 min to create a block[7] .Therefore ,there is a challenge to handle the variable number of transactions in allotted i.e. if Block chain Technology wants to carry many number of transactions ,the size criteria of the block chain need to be solved[7].

XV. BANDWIDTH

In given Fixed Time interval data can be transmitted [4].Utilization of small bandwidth will lead to handle more number of transactions. Near about 400-500 transactions can be handled in one block [5].

XVI. REUSABILITY

API services of Bitcoin need to be developed for reusability purpose.API services should me more user friendly API for Block chain [6].

XVII. FORK

step where blockchain is divided in two chains for some static purpose or dynamic purpose .In blockchain technology protocol software services changes the phases of old blocks/nodes to new blocks[7],[8].Fork situation can reduce due software changes,algorithm changes,Network changes,change in interface,services,technology,method ,operating system,Administration,Setting versions,features,limitations,protocols[7],[8].

Considering the change in input and output, the fork is split in two types called as Hard Fork and Soft Fork [7],[8]. Sometimes fork can lead to confusion between developers, miners involved in it which may lead to situation of debate for the correct decision to be done [7],[8].

Example: Segwit2X-Hard Fork concept for the Bitcoin Blockchain in 2016-2017[7][8].

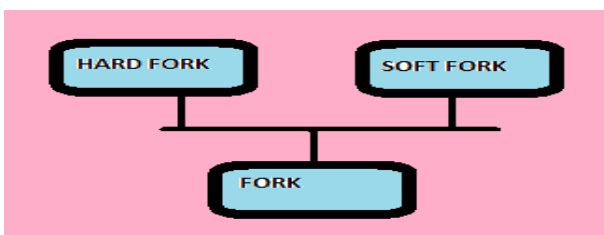


Fig 3: Types of Fork.

A hard fork –dynamic change from the old ones of the Block-chain ,and process executing old versions will not be overcome by the latest version[7],[8]. A Hard Fork consists of a minute change of phase from old phase to new phase making old versions of process invalid or invalid transactions[7],[8]. In case of Hard fork block is accepted even if the block is not in chain but has followed all protocols[7][8]. All process/nodes have to update with new technology of the software protocol if want to continue with recent fork chain, which leads to creation of fork in the Blockchain, one channel leads to the new, updated Blockchain and other channel leads the old Block chain[7],[8]

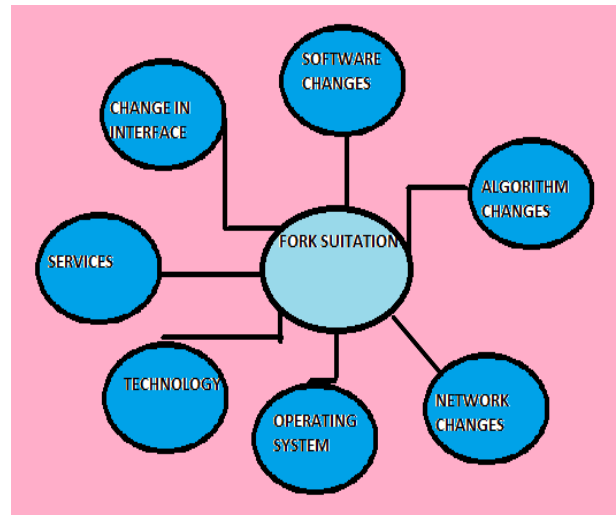


Fig 4: Situation in Fork.

Lot of change in both the forks Hard Fork and Soft Forks will result in lack of consistency in a cryptocurrency[7],[8].Sometimes-Hard Fork-some crypto currency has same name as that of original ,leads to merge with original currency brand[7],[8].

For Example: Hard fork –Block size –range from 4MB to 2MB ,Bitcoin cash, Lite coin , Ethereum, and Bitcoin Gold both are different still leads to merge with each other leading to fake.

Soft Fork: Soft Fork is compatible with old blocks/invalid transactions [7],[8] .It is opposite of Hard Fork. Soft Fork works if there is temporary change in the transaction .Post Soft Fork is compatible with Pre Soft Fork [7], [8].

For Example : The soft Fork limits the block size to 2KB,initially set to 2MB i.e. the blocks whose size is greater than 2KB will be rejected in the new chain after new version[7][8].



Fig 5: Conversion of Soft Fork.

XVIII. TIMELINESS

Proof that the time of the digital signature was in fact the actual time [16].

XVIII.PARTIAL PRIVACY

All changes done on the Block chain can be traced back to a particular/user [6].

Limitations of Blockchain Technology with its Applications

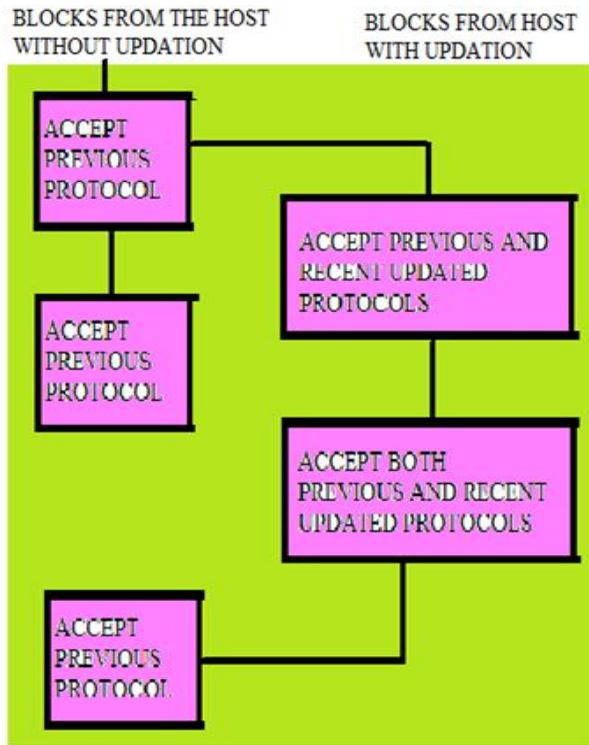


Fig 6: Fork Protocol.

XX. HIGH ENERGY CONSUMPTION

Power Consumption is required for maintaining a real-time ledger [8],[9]. New Node gets created and communicates with each and every node. This creates transparency [8],[9]. Essential amount of power is required to validate transactions. Every node results in fault tolerance, ensures zero downtime, no change, time to store data on Blockchain, transactions, processing, Hash Value, private key, Public Key, signature verification, validation [8],[9]. All these need power consumption and time. Some process is repeatable leads to wasteful of gain consensus [8],[9].

Validation of seal process is done block chain Technology; this requires high power consumption [9].

XXI. EQUILIBRIUM BETWEEN NODES QUANTITY AND AFFORDABLE COST

Nodes lack in low quantity size. In such case, leads to high cost and nodes receive more power but the transactions processed till end are slow, which result in situation of low intensive work [12]. There are many times tampering schemes with different security issues [16]. For authentication of timestamp, the verifier uses the public key which is open source. Blockchain Engineering requires huge initial investment [8].

XXII. ADAPTATION OF EXISTING INFRASTRUCTURE

Participants get used to a more peer-to-peer Network (decentralized Network) [1].

XXIII. VALIDATION TRANSACTION

With respect to particular blockchain state of it is well formed and if the output it attempts to spend existing in the

state and if condition is satisfied in that condition is satisfied in those output [6]. The transaction may or may not be valid with respect to a different block chain state [6].

XXIV. REGULATORY NONCONTINUOUS

EU authorities are only exploring the regulatory impact of Blockchain application to virtual currencies [6].

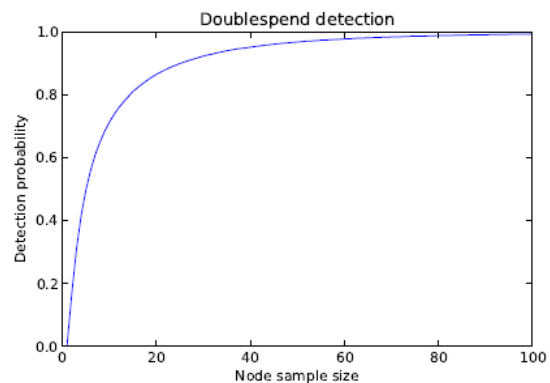
XXV. HIT OF FIFTY ONE PER CENT

This problem is raised when 2.0 miners are finding value of hash block at same instant of deadline and coming to approximately output. In such situation, Blockchain is divided in 2.0 various chains which is granted as authenticate [10],[11],[12].

2.0 SPENDED PROBLEM

Large number of nodes in connection with Network doing only one transaction, possibility of double spent is minimized. It is also observed that distributed nodes in connection with network, can also be used to avoid the Double Spending in chain of Blocks [10],[11],[12]. The chain is split into two to invest money one more time. Rejection mode of Digi, cash or crypto-currency schemes, when it is highly accept a only one digital token multiple number of times [10],[11],[12]. Bitcoin helps against double pended problem by authentication, every one transaction in queue of the chain of blocks to confirm that inputs taken for the transaction have not utilized hence before [10],[11],[12].

The potentiality of Two-spending trial is succeeded in connection to the nodule sample size of the client.

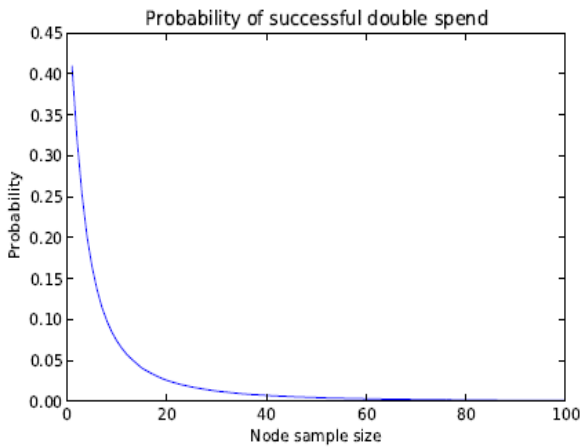


Graph 1: The potentialities of the client detect a 2.0 hit.

XXVI. SIBYLS HIT:

The Network cannot validate the existence of machines. This attack is occurred when same node enables multiple element [10],[11],[12]. This attack causes Blockchain to activate all nodes in chain which are under its authority. It can cope up with the last 2 attacks with special capability of all transactions with related algorithmic program [10],[11],[12]. Since dispersed consensus technique avoids hack [10],[11],[12].





Graph 2: Potentiality of succeed 2.0 spend

Data Accumulation, surveillance systems are tractable to hacker, penetration and violations [6]. One and all transactions occurring in nation of miners need to be certified, exit bogus transactions incapable for entry of public certification and endorsement [6].

Since chain of Blocks is continuously under supervision by complete netting of client, every one holes the replica of Block chain, evils in no way put in fake blocks into the common log without urgently being noted by others.

Since Blockchain protect secrecy and confidentiality the authentication of benefits is depended upon the safe secret keynote, in the way of online digitize uniformity [8]. No other members can retrieve once safe secret keynote is gained or steal away [8]. Accordingly all credit client hold in the chain of Blocks disappears and it is highly not possible to recognize the pirate [8]. This impact may be highly destructive to integrity steal which are disconnected, where involvement of other member organizations or fundamental bodies [8]. Secure mode exchanges, authority threat, identify, suspect actions, or help find culprits [8]. However this does not mean that it can resist any types of fake and oppose number of verities of fake and hack. This process is identical to correct the security seller[14]. Block chain process is very powerful technique in avoidance of data fake, like process lease process fake, where fake data is found[13]. This process is very powerful technique avoiding poor whispering, whitening hit, since they are very few polling filler consideration of **Sibyls Hit**, contiguous hit and mask hit [13].

Therefore, it's difficult to agree for excellence of logs in the Blockchain. Many more logs damages the huge variety of other net prints make availability of trusty backing and rewrite the cracked edition.

The log is accessible to the general public and confirmed lock, close to rejecting the ability for fake. When a client does confirmation of bitcoins, by client charging the bitcoins, the vendor is fully assured that negotiation will continue and there are no any chances of costing fake.

XXVII. SOME EXAMPLES-APPLICATIONS OF BLOCKCHAIN TECHNOLOGY

Emerging new innovations for distributed log organization and recent chain of block Engineering is used in companies like soft bank, IBM, blue chip brands-SAP, BP, Samsung, shipping giant.

Diamonds are Everlasting-Persistent: Diamond supply chain can be formed to avoid fake and illegal marketing [15]. Ever-log keeps track of whole gem from mine lying to customer. This process will be helpful for us to settle the real cost effective, conditions, organization obstacle [15]. It's an authentic share. It is one of the designs to plot Block chain based registration of every one endorsement gem in the universe [15]. In short Blockchain is a solvent to imperative issue [15].

IBM Blockchain: Familiar with raw materials used to delivery is bit complex and working phase of one and all accessories and its reputation, standby known.

Government: Many governance institutions have expressed an attention in Block chain engineering to store open registry on a distributed information handling system [15]. Block chain permits metropolitan and countrified peoples everywhere Finn to get logs [15]. Many others include governance applications like schooling field, open registry and voters' duplication of record [15].

Waste Management: The enterprise will help us to activate surveillance of avoidable stages to modify functional capability and refine assets [7].

Taxation: Blockchain access control, Real time data, openness-features because of which Blockchain Engineering can be used in Taxation[15]. Blockchain Technique makes fake and fault more easier to analyze, since the process gives neat clear and pure data regarding process and data in online process [15]. Its beneficial to keep track of VAT when and where paid, reducing VAT fake [15].

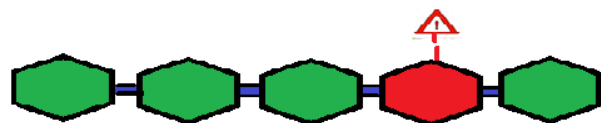


Fig 7: Fake detection in Blockchain Technology.

Insurance: This enterprise will help the user to avoid fake transactions and keep logs on mark [15].

Voters Identification: Block chain enterprise to record locals citizens identity, working mode to involve in real time poll and proof their residence [16],[30].

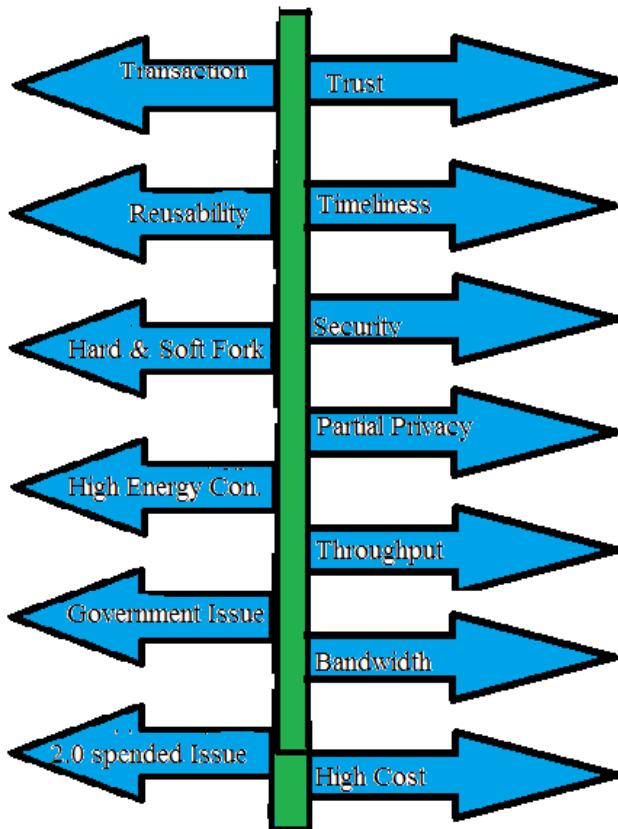


Fig 8: Limitations of Block chain Engineering

Land Registry: Block-chain Engineering is not only relevant to the crypto organization and by medium scale, small scale organizations. The governance uses it to enroll land records. Blockchain organization is form designed combined with online data organization of the National Agency of Public Registry (NAPR). Using Blockchain is advantageous since it is transparent and fake registry can be reduced or most avoided.

Smart Cities: The Block chain Engineering is point-to –point technology, spreader log organization to record everyone process carrying internally in netting. Emergency ICT Engineering in Block chain Technology which in builds recent varieties of chances proving the openness and associate number of varieties of uses required for achieving the working of energy consuming[16]. The Block- chain based Engineering is an emerging tool for authentication, validation technique for virtual currencies but more research utilize this technology to be useful in variety of appliances[16].

The prime prototype has operated since last from few years ,yet including the raise of the more volume of record swapped during the process ,this lead for the servers the problem of congestion and unique point of flop ,so as to reduce fake hits. The Blockchain is skilled to create extremely safe, alone, speeded program [16].

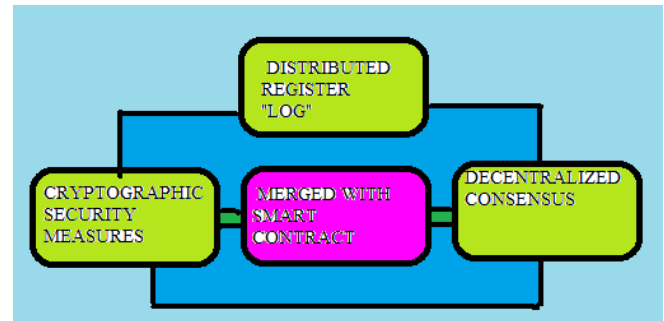


Fig 9: Functioning of Smart Cities.

Medical Aid: Pharmaceutical files are spread and incorrect, with incompatible information processing i.e. clinic, wards are usually bound to operate with corrective or defective tolerant data i.e. make it easier records exchange while delivering confirmation and continuation in confidence [6].

XXVIII. CONCLUSION

This paper summarizes the most efficient utilization of the Blok chain Technology in various fields like Diamonds, Health Care, Land Registry, Education, Smart Contract, IBM, Governance Organization, Waste Management, Income Tax, Insurance, Smart Cities, Ballot Polling, Pharmaceuticals Industry and many more applications.

There is no third party involved in it i.e. point-to-point communication. Some possible limitations of Block chain is proposed. Block chain Engineering depended applications are raising now a days and we blueprint deep survey on Block chain depended applications in upcoming years. We can say that there can be variety of models for the Block chain Technology i.e. it is related to all segments of society and solution for all human lives.

REFERENCES

1. A. Bahga, V. Madiseti, “Blockchain Platform for Industrial Internet of Things”, Journal of Software Engineering and Applications, No. 9, pp. [36]533-546, 2016.
2. Sarah Underwood. Blockchain beyond Bitcoin. Commun. ACM, 59(11):15–17, October 2016.
3. A. Litvinenko, A. Āboltiņš, “Computationally Efficient Chaotic Spreading Sequence Selection for Asynchronous DS-CDMA”. Electrical, Control and Communication Engineering, vol.13, pp.75-80, 2017.
4. Yuanfeng Cai and Dan Zhu. Fraud detections for online businesses: a perspective from blockchain technology. Financial Innovation, 2(1):20, 2016.
5. Antonopoulos AM. Mastering Bitcoin: unlocking digital cryptocurrencies. ^ O’Reilly Media, Inc.^; 2014.
6. Blockchain technology, “Advantages & Disadvantages of Blockchain Technology” [online]. 2016. Available from: <https://blockchaintechnology.com.wordpress.com/2016/11/21/advantages-disadvantages/>.
7. J.Light, “The differences between a hard fork, a soft fork, and a chain split, and what they mean for the future of bitcoin” [online]. September 2017. Available from: <https://medium.com/@lightcoin/the-differences-between-a-hard-fork-a-soft-fork-and-a-chain-split-and-what-they-mean-for-the-769273f358c9>
8. W. Fauvel, “Blockchain Advantages and Disadvantages” [online]. August 2017. Available from:

- <https://medium.com/nudjed/blockchain-advantage-and-disadvantages-e76dfde3bbc0>.
9. Bitcoinwiki; 2015. Accessed: 24/3/2016. <https://en.bitcoin.it>.
 10. A. Bahga, V. Madiseti, "Blockchain Platform for Industrial Internet of Things", Journal of Software Engineering and Applications, No. 9, pp. [36]533-546, 2016..
 11. Sarah Underwood. Blockchain beyond Bitcoin. Commun. ACM, 59(11):15–17, October 2016.
 12. W. Fauvel, "Blockchain Advantages and Disadvantages" [online]. August 2017. Available from: <https://medium.com/nudjed/blockchain-advantage-and-disadvantages-e76dfde3bbc0>.
 13. Swan M. Blockchain: Blueprint for a New Economy. a O'Reilly Media, Inc.; 2015.
 14. D. Balaban, "Blockchain Networks: Possible Attacks and Ways of Protection" [online]. Available from: <https://resources.infosecinstitute.com/blockchain-networks-possible-attacks-ways-protection/#gref>.
 15. J. Golosova, A. Romānovs, "Overview of the Blockchain Technology Cases". In Proceedings of the 59th International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS), October 10-12, 2018, Riga, Latvia. IEEE, 2018, pp.1-6. ISBN 978-1-7281-0098-2 .
 16. MedRec, "What is Medrec?" [Online]. Available from: <https://medrec.media.mit.edu/> .
 17. Akif Khan. Bitcoin payment method or fraud prevention tool? Computer Fraud & Security, 2015(5):16 – 19, 2015.
 18. DHL Trend Research, "Blockchain in Logistics", 2018.
 19. Gillis, M.: Tax Reform and the Value Added Tax: Indonesia. World Tax Reform Case Studies of Developed and Developing Countries. ICEG, pp. 227–250 (1990).
 20. N. Szabo, "The idea of smart contracts," 1997.
 21. A. Litvinenko, A. Aboltniš, "Computationally Efficient Chaotic Spreading Sequence Selection for Asynchronous DS-CDMA". Electrical, Control and Communication Engineering, vol.13, pp.75-80, 2017 .
 22. Republic of Estonia E-Residency, "The new digital nation" [online]. Available from: <https://e-resident.gov.ee/>
 23. Sarah Underwood. Blockchain beyond Bitcoin. Commun. ACM, 59(11):15–17, October 2016.

AUTHORS PROFILE



Ammbika V. M Completed Bachelor of Computer Science And Engineering in 2005 from Shivaji University with First Class and Distinction, Completed M.Tech in Computer Science and Engineering from JNTU University with First Class and Distinction, Doctoral Research Scholar in Computer Science And Engineering from Koneru Lakshmaiah Education Foundation (KLEF), Vaddeswaram, Guntur District Andhra Pradesh-522502, India., Published papers -1: "Security Challenges with cloud computing" in IJEST, Volume 4, Issue 10, 15 Oct. 2015, 2: "Computer Security with computer protection and network management" in IJESRT volume 5, Issue 6, 05 JUNE 2017, 3: "Bigdata with Internet Of Things (IOT)" in IJEST volume 06, ISSUE 6, 05 JUNE 2017, 4: "Balancing Load using parallel computing and distributed computing", in IJESRT volume 07, Issue 4, 05 April 2018, membership-Member of Indian Institute of Engineers of India MIE-1538225, Member of ISTE –LM-123599 .

Dr. D.S. Rao, PhD, is an Associate Professor (CSE) and Associate Dean (Planning & Development) at Koneru Lakshmaiah Education Foundation (KLH Deemed to be University) at Hyderabad, India. He received his Ph.D. from National Institute of Technology, Rourkela (Soft Computing Techniques) and M.Tech (Computer Science & Engineering) from JNTU Hyderabad, India in 2018 and 2012, respectively. He has more than twelve years of professional experience in information systems, security policies and technologies. His research interests include noise prediction, frequency analysis, noise mapping, and development of soft computing models, computer forensics, block chain technology and GPS. Dr. D.S. Rao has published numerous articles in refereed international journals and conference proceedings including Sage, Inderscience, Elsevier, Springer, IEEE and JUOEH. He is an associate member of INCE USA and is serving as associate editor, editorial board member, reviewer of several journals of international repute