International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-7 Issue-5, January 2019

Success of Blockchain and Bitcoin

Chirag Madan, Aayushi Sinha, Kamlesh Sharma

Abstract: ***Block chain technology in today's time changing the world of transactions and documentations. Mainly it gives a transparency to the numerous fields like electronic voting, cost analysis of product manufacturing, paying employees, cloud storage and smart contracts (the economist). Or we can say that these applications are the major pillors of a country which can be handled very efficiently with the help of blockchain technology. This paper explains the role of blockchain in bitcoin and will give the applications of blockchain In the field of transactions, governance, productions and documentation. The use of blockchain will reduce the use of third party and third party databases. The paper will give the relation of bitcoin and blockchain technology for improving the political aspects of country and reducing the dominating behaviour of the powerful persons and frauds in various fields by giving the transparency.***

Keywords: ***Transactions; Governance; Productions Component; Blockchain.***

I. INTRODUCTION

Blockchain are originally the database of colletion of blocks containing the details of transactions between the two parties. The blocks are interconnected with each other and having the specific timestamp it is the form of p2p (peer to peer) communication. once the transactions are stored completely in the blockchain database then it became impossible be reversed or changed. These can be understood as an open and distributed ledger that is cpable of recording transactions between two parties efficiently and in a verifiable and permanent way. Programming of this ledger can be carried out so that transactions can be triggered automatically. This technology has the ability to reduce the usage of the most powerful feature of the current transaction method i.e the Middle man. It allows people to transfer a unique piece of digital assets or data to others, in a safe, secure, and irreversible way, this technology can create: digital currencies that are not backed by any governmental body,smart contracts whose execution does not require any human interference. As we all know that digital money has attracted a considerable amount of people and services with the help of digital ledgers.

Revised Manuscript Received on 30 January 2019.
***** Correspondence Author
Chirag Madan*, Students, Department of Computer Science and Engineering, FET, Manav Rachna International Institute of Research and Studies, Faridabad (Haryana), India.
Aayushi Sinha, Students, Department of Computer Science and Engineering, FET, Manav Rachna International Institute of Research and Studies, Faridabad (Haryana), India.
Dr. Kamlesh Sharma, Associate Professor, Department of Computer Science and Engineering, FET, Manav Rachna International Institute of Research and Studies, Faridabad (Haryana), India.

It has a potential impact on the majority of transaction related practices that the transaction processes like loans, bonds, stockseverything has been digitalized but the main problem is that the fee taken by the middlemans like banks, financial firms ,etc. blockchain technology and bitcoin tends to solve this problem by providing the p2p transaction process. Blockchain technology has created the backbone of a new type of internet by providing the ability to distribute the information digitally but not copying.

It was originally devised for the digital currency, Bitcoin, but tech community is now finding other potential uses for the technology. Bitcoin is popularly known as digital gold. To date, the total value of the currency is close to 9 billion.

- Protocols used in blockchain are as follows;-

A. Ethereum

The major feature of Ethereum is that it is a public, open-source and block chain oriented distributed computing protocol that characterizes sensible contracts practicality. This protocol has served with a a redistributed virtual machine referred to as Ethereum Virtual Machine(EVM), that carried out dynamicalthe whole with the help of a worldwide network that contains public nodes and therefore the token referred to as ether, it's to boot explicit as gas. It area unit typically applied for preventing the spam on networks. Bloomberg explains Ethereum as shared code that is used by all; but, it's unalterable. Ethereum is to boot used as a protocol for localized applications, wise contracts and localized autonomous organizations, with kind of functioning applications developed on that by March 2016

B. Ripple accord Network

The Ripple dealings Protocol (RTXP), waqscoined in 2012, it's been developed on the thought of academic degree ASCII text file distributed accord ledger, net protocol, and native currency termed as XRP or ripple. Ripple helps in facultative the instant, safe and nearly gratuitous world cash transactions of any level (either higher or lower) with none chargeback. The protocol is embraced having the power to support tokens presenting crypto currency, act currency, unit and therefore the selection value unit like mobile minutes, frequent flier miles etc. By the tip of 2017, Ripple is anticipated to be the third-biggest crypto currency in terms of capitalization, once the bitcoin and ether. Hyperledger.

C. Hyper Leadger is to Boot Associate Degree Open Provide Blockchain Platform,

Initiated in 2015 by the operating system Foundation, to support the blockchain-based distributed ledgers.

This protocol primarily focuses on ledgers developed to support international business transactions, job leading cash, technological and supply chain businesses, it's having the target of rising many performance and responsibility standards. This protocol emphasizes on creating combined efforts for creating open standards and protocols, by providing an everyday framework that backs varied elements for various uses, in conjunction with a range of blockchains having their own storage and agreement models, and put together the services for access management, contracts and identity.

D. D. R3's Corda

Corda is started by R3 Company it's a distributed ledger protocol that has been developed from all-time low up for recording, management and synchronizing the money agreements among regulated money establishments. It is, by plenty, excited by, and captures the benefits of blockchain systems, with no vogue picks that flip blockchains unsuitable for heaps of banking things. Corda's vogue came up as results of great analysis and prototyping with team members. it's presently associate degree open sourced protocol since the code matured any.

E. Symbiont Distributed Ledger

This protocol was declared in Gregorian calendar month 2016 as a code development kit for the Assembly, that is that the permissible distributed ledger a section of Symbiont's wise contracts system. Assembly is taken into account as a results of the initial distributed ledger acceptable for institutional finance. it's a greatly secure, high discipline Byzantine fault-tolerant distributed ledger, that could methodology a sustained eighty,000 transactions each second throughout a} terribly native multi-node network. As declared by Co-founder of Symbiont, localized systems have to be compelled to now not be slow and with Assembly, it's been completed.

Advantages of BCT can be broadly classified as

The fig. 1 is discussing the advantages of BCT.

- **Immutability**

Anything once stored in the blockchain can't be altered due the network issueor any other malfunctioning .once saved in blockchain always stays in blockhain.

- **Permanence**

As said once saved in blockchain always stays in blockhain. means that a public blockchain will appear as the public leadger means that till the time blockchain remains operative the data on blockchainwill be accessed at any point of time

- **Removal of Intermediaries**

Blockchainoperates on the concept of point to point transaction which reduces the need of third party or the intermediate brokers which enables the higher speed of transaction moreover secure.

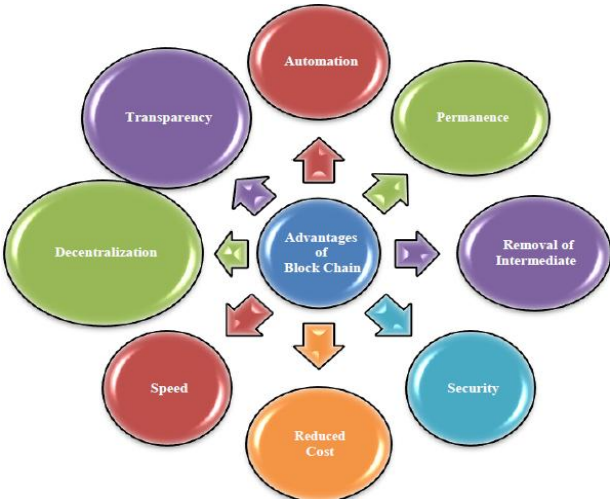

Fig.1. Advantages of Block Chain

- **Automation**

Block chain provides automation in the process of storage because it removes the third party interference and the distributed ledger are updated in real time by miners, which enables the automatic transition and storage of the data.

- **Decentralization of consensus**

There is no as such central authority for clearing the transaction validation; in blockchain the effort to complete a transaction is widely distributed between the miners.

- **Speed**

Everyone today is concerned about the speed of transaction. Blockchain effectively solves this problem.

- **Lower Costs**

As discussed earlier blockchain removes the third Party which defnately reduces the overall cost included in the process.

- **Near-Impossible Loss of Data**

Each miner participating in the process contains a full copy of ledger contained in the system which helps to step up the features of data storage and security which makes it impossible to lose the data stored in the system implemented using the blockchain technology.

- **Security (Encryption Through Cryptography)**

And now comes the most important advantage of the blockchain which is given by the principle of blockchain and public key and private key cryptography neither the nodes nor anyone else except for the sender and the recipient can access the data sent across the blockchain.

II. ESTONIA`S EXPERIENCE IN BRINGING BLOCKJCHAIN CLOSER

In 2015, Estonia announced itself as a leading country in the development of Blockchain-based services. It is remarkable that not only the commercial sector but also the government, giving the go-ahead for Govtech developments, has become interested in this technology: Public Notary (based on the already operating electronic residency system) and the project on transferring medical records of Estonian citizens into the Blockchain.[1]

Public Notary is an "electronic version" of a notary with remote access from anywhere globally. It was designed by developers of the e-Residency project, allowing foreign citizens to establish a business within Estonian jurisdiction.

E-Residency creation was preceded by several years of digitalization and IT sector development. The country's whole territory provides access to high-speed Internet and its socio-economic environment is quite attractive for highly experienced programmers from Belarus, Ukraine, Russia and even Finland. Specialists from the EU and US countries are also frequent guests because of low taxes.

As to further Blockchain implementation in the e-Residency project, it is Kaspar Korjus who focuses on this issue. He is a young engineer qualified by Megan Smith, ex-vice-president of Google, as one of 20 global digital technology leaders.

"There is no better place for Blockchain discussions than here in Tallinn the home of digital society. Blockchain itself is nothing, it needs to be considered together with digital identity, legal environment and efficient e- governance. Only then the system will start to understand its real impact," says Korjus. Parallerly the e-health foundation of Estonia has decided to switch all their data to the blockchain to make it more secure and transparent.

The system will secure citizen health data storage and allow to monitor patient conditions in real-time. LHV Pank, which has developed the Cuber Wallet mobile application, focuses on Blockchain implementation in the banking sector. In 2015, LHV customers got an opportunity to transfer money safely for free using the Blockchain.

In January 2017, the Estonian subdivision of Nasdaqhas succeeded in testing the voting of stakeholder in the private companies and is planning to implement the concept in public domain also.

III. PRINCIPLE OF BLOCK CHAIN

A. Open Ledger

In open ledger we are having a centralized place where each of the transaction is being stored and every other transaction is being linked to it. With the concept of open ledger system can concede:-

- Where the money is—As there are many blocks of each transaction that are generated and each one is having record of all the transaction that are there in the whole process therefore one can easily able to track where the money is .
- How much money does one have—After a certain transaction one it can be easily visualised from the blocks that how much does one is having.
- Everyone can decide whether the transaction is valid or not---After visualising how much money does one have it is very easy to confirm that the particular transaction is valid or not in the context to which it is done.

Disadvantage of open ledger is that there is a centralised place in which all the transactions records are being stored but as the block chain tend to remove that centralised place therefore to overcome that system are using a new principle called DISTRIBUTED OPEN LEDGER as In distributed open ledger instead of having a centralised block system can distribute the block of transactions to every node in a network and all the nodes receive the same copies of that Block.

IV. BLOCKCHAIN IN FINANCE

The fig. 2.shows use of Blockchain in Finance

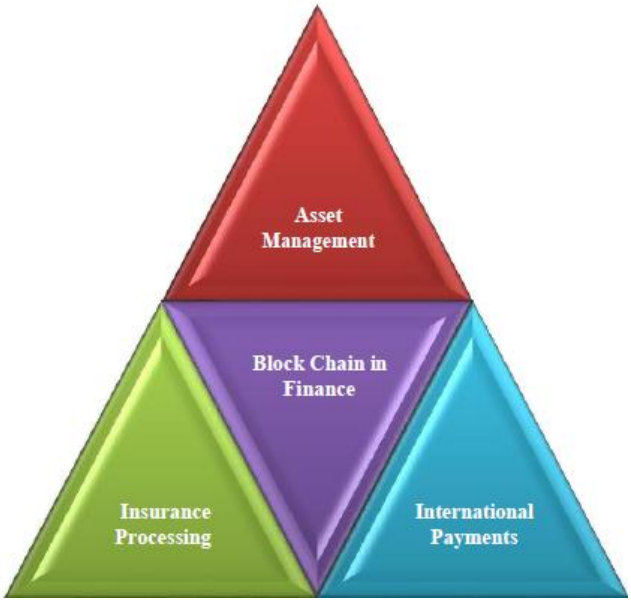

Fig.2. Block Chain in Finance

A. Asset Management

Asset management with Traditional trade processes may not be as swift as it need to be or might be manual and can be filled with risk when reconciling and matching – these things can be difficult in terms of cross border transaction and for non-standard investment products, e.g. loans. The middle persons and brokers keep their copy of transaction which can create inconvenience and errors.

Blockchain technology would help in making process entirely streamline by providing an automated trade lifecycle. This would result in substantial decline in infrastructural cost, efficient and effective transparency and data management moreover faster processing cycles.

B. Insurance Processing

Some great challenges of insurance sector can be listed as Fraudulent claims, manual processes, fragmented data sources which leads to the reduction of customer satisfaction. Creating policies in the form of smart contracts based on blockchain helps in insurance. It offers complete control, transparency and traceability for each claim and could lead to automatic pay-outs.

C. Global Payments

The global payment sector is huge yet it is slower, costly and highly prone to errors which makes it untraceable leading to money laundering. The blockchain reduced the time of money transfer to other countries by providing the real time payment transfer.

D. Compliance

Financial establishments across the planet area unit answerable for obliging and reportage on variety of needs from their native regulator. grasp Your client (KYC) maybe key demand here however the method will be unbelievably time overwhelming and lack the automatic client identification technology and integration required by groups to expeditiously do their work.

Blockchain technology may give a digital single supply of ID data permitting the seamless exchange of documents between banks and external agencies. This might possible lead to automatic account gap, reduced resource and price, all while maintaining the privacy of knowledge that's lawfully needed.

V. SECURITY ASPECTS OF A BLOCKCHAIN DEPLOYMENT

BCT provides a secure and naturally decentralized model for dealing processing. By appropriate use of cryptographic key , confidentiality of dealing can be addressed, This shuffling blocking chemical chain arrangement robust. Due to legal and technical foul vexation, institutions that operate financial book or registries may be inclined to utilize permission blockchains as they form a more command and predictable surround than permission less blockchains. Blockchain systems typically need to look at certificate from the following position:

A. Smart Contract Security

This is essentially used for authentication. Membership to the blockchain must be restricted to player UN agency are content to needed scrutiny. The block chain net should make sure that solely legitimate entities ar allotted the desired certificate. All dealing initiated from member nodes got to be signed in order that solely valid player will produce one sense of dealing within the network

B. Network Level Security

It is counseled that communication between parts of various nodes is formed secure from a networking point of view. The network should be proof against many alternative attack vectors i.e., each external and internal to the network.

C. Transaction Level security

It is terribly vital for monetary establishments to keep up the dealings accuracy and changelessness. The dealings model should be specified company having access to the ledger don't seem to be ready to trace activities or Synonyms/Hypernyms (Ordered by calculable Frequency) of noun dealings done by alternative participants by observant dealings addresses. Transactions ought to be unmodifiable i.e. nobody ought to be ready to amendment the payment total , the sender information , the recipient info or the other associated dealings info.

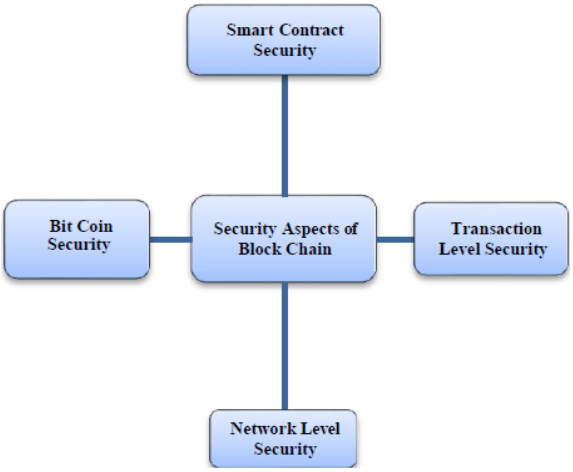

Fig.3. Security Aspects of Block Chain

D. Bitcoin

Fig 3 shows the security aspects of blockchain that relates with bitcoin transactions there is no need for any further processing. Bitcoinesareimmediate, fully automated and very secure than other processes. The whole process behaves almost as if Alice gave Bob a 1$ bill first and then Bob handed it over to Zoe at a later time. The main difference is that in the case of physical cash, there is no need for proving cryptographically that Bob or Alice owns the cash. Physical possession of cash is the proof, while in the world of bitcoin digital currency, the 'possession of bitcoins' needs to be proven and verified cryptographically at the time when it is 'virtually handed over' to the next bitcoin address.

Although bitcoin-based payments avoid the need for settlement, they are currently having several orders of magnitude lower transaction processing throughput than the payment card-based systems, due to being completely public and open to everyone's participation. All that must be managed with fairly complex consensus algorithms involving brute force proof-of-work, puzzle-solving calculations, etc.

VI. HOW WILL MINING TAKE PLACE

Masses expanse unit causation bitcoins to every different over the bitcoin meshwork all the time, however unless somebody keeps a record of of these dealing , no-one would be ready to keep track of United Carry Nation agency had salary what. The bitcoin network deals with this by aggregation all of the proceedings created throughout a chemical group amount into an inventory, referred to as a block. It's the mineworker' business to substantiate those proceedings, and write them into a book. [3]Making a hash of it.Fig.4 shows the hash cycle of block chain.

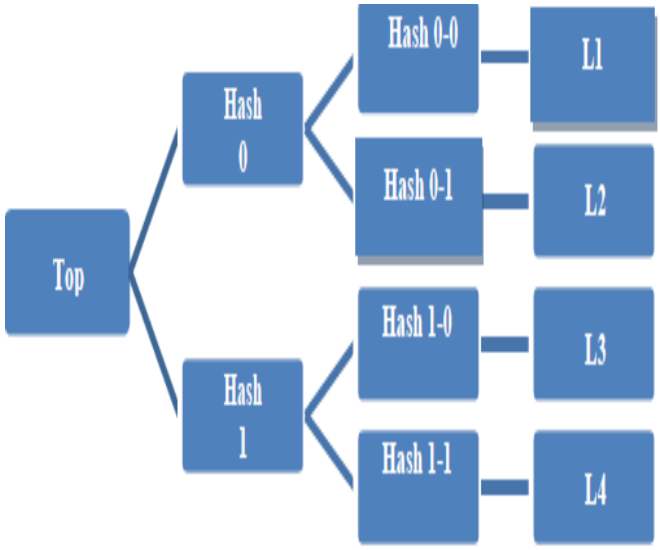

Fig.4. Hash of Block Chain

Whenever a brand new blockage of transaction is formed, it's else to the blockchain, making associate progressively extended list of all the transactions that ever happened on the bitcoin network. A perpetually updated written matter of the block is given to everybody United Nations delegacy participates, so they recognize what's happening . But a book should be trusty, and every one of this is often control digitally. however will system have a tendency to take precaution that the blockchain Synonyms/Hypernyms (Ordered by Estimated Frequency) of noun stay intact, and International Relations and Security Network 't tampered with? this is often wherever the miner are available in.

When a block of transactions is formed, miners piazza it through a method. They take the data within the block, and apply a mathematical formula to that, turning it into one matter else. That one thing else could be a so much shorter, apparently random sequence of missive and numbers game called a haschisch . This haschischish is cargo deck on along side the block, at the top of the blockchain at that time in time. Hashes have some fascinating dimension . It's straightforward to supply a hash from a set of info variety of a bitcoin block, however it's much not possible to pattern out what the entropy was simply by gazing the hash. And whereas it's terribly straightforward to supply a hash from an outsized amount of information, every hash is exclusive. If system alter only ace type in a very bitcoin block, its hash can amendment fully. Miners don't simply use the transactions in a very block to get a hash. another point of information area unit used too. one amongst these point of information is that the hash of the last block hold on within the blockchain. Because every block's hash is make using the hash of the block before it, it becomes a digital version of a wax seal. It confirms that this block – and each.

VII. ADVANTAGES OF BITCOIN

There is no fee to receive bitcoins, and many notecase let system control how large a fee to pay when expenditure. Most wallets have reasonable nonpayment fee , and higher fees can encourage faster confirmation of your transactions. Fee are unrelated to the sum transferee , so it's possible to send 100,000 bitcoins for the same fee it costs to send 1 bitcoin.

A. Protection Against Fraud

Any job that accepts credit cards or PayPal is attentive to the matter of payment that square amount later reversed. Chargeback frauds result in restricted market place reach and increased prices, that successively penalizes customers. Bitcoin payments square measure irreversible and secure, that Synonyms/Hypernyms (Ordered by Estimated Frequency) of noun mean that the value of fraud International Relations and Security Network 't any personpushed onto the shoulder of the merchandiser .

B. Fast international Payments

The simplest thing is to transfer funds in the form of bitcoins because there is no need of the banks or third party and no extra fee is included.

C. No PCI Compliance Required

Accepting credit cards on-line usually needs in depth security assay so as to adjust to the PCI customary. Bitcoin still needs system to secure your pocketbook and your payment asking . However, system are doing not carry the prices and responsibilities that bodyguard process medium information from your client like mastercard telephone number .

D. Get some free visibility

Bitcoins have gathered a good visibility in market this allows the customers to spend the money in form of bitcoins which is definitely beneficial for the market growth also.

E. Multi-signature

Bitcoin conjointly includes a multi-signature feature of speech that permit bitcoins to be spent as long as a solidifying of a bunch of individuals authorize the dealings. this could be utilized by a board of executive to forestall any extremity to create expenditures while not enough consent from different members, yet on runway that members allowed every payment .

F. Accounting Transparency

Many organizations area unit needed to supplying accounting system papers regarding their activity. victimization Bitcoin permits system to supply the very best level of transparency since system will be able to give info your members can use to verify your balances and transactions. Non-net income organizations can even enable the superior general public to envision what proportion they receive in contribution.

VIII. HOW BITCOIN HELPS TO AN INDIVIDUAL

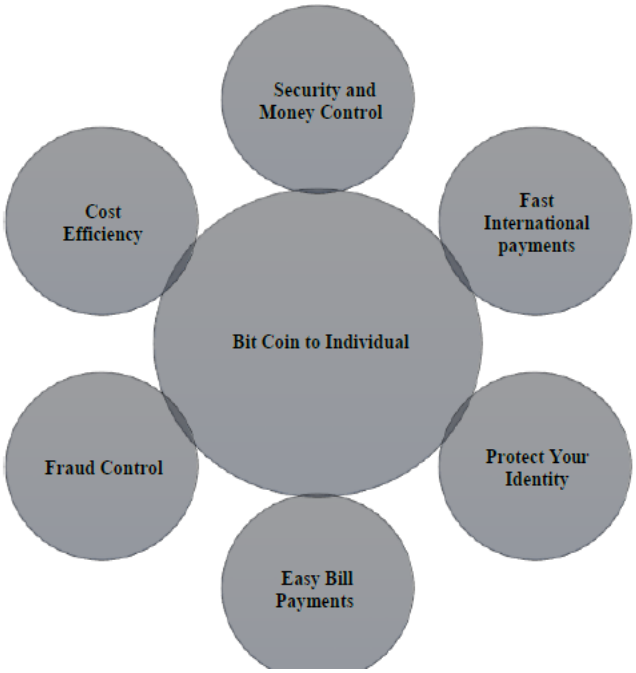

Fig.5. Bitcoin to Individual shows the cycle of bitcoin to individual.

A. Individuals Mobile Payments Made Easy

Bitcoin on mobiles permits system to pay with straightforward II step scan-and-pay. No need to swipe your card, character a PIN number, or sign something. Receiving a bitcoin payment is just simple. All system need to do is just show your OR code to the payee and with the single click of a button the payment is instantly transferred.

B. Security and Control Over Your Money

Transactions of bitcoins are secured by military gradation cryptography. No one is having the authority to create the payment detail on their behalf. It has specified steps to guard your pocketbook. Bitcoin will provide system with management over your cash and a robust horizontal surface of protection against fraud.

C. Fast international payments

Sending bitcoins across borders is as straightforward as causation them across the road. There is no bank upon which system have to depend upon, no fees for creating a worldwide transfer, and no special limitations on the minimum or most quantity you'll send.

D. Protect Your Identity

As there is no virtual debit and credit card therefore problems of identity theft are not there .In fact, it is even possible to send a payment without revealing your identity, almost like with physical money. System should however take note that some effort can be required to protect your privacy.

E. Control Against Fraud

It provides user with unprecedented level of Security. Protection against most prevalent frauds like chargebacks or unwanted charges, and bitcoins are impossible to counterfeit.Complete Encryption and Secure Decryption of user wallet make it difficult to steal user identity. Bitcoin is designed to allow its users to have complete control over their money.

F. Global Accessibility

Bitcoin can help to make money transfer interoperable. It helps banks, business or individual to securely allow the transaction of payments anywhere at any point of time, irrespective of a bank account.But still Bitcoins are away from the various countries due to their own limitations.

G. Cost Efficiency

Bitcoins allow the cost efficiency because there is no middle man included in the transaction which helps to allow the transactions with no or minimal transaction fee. it can help to reduce poverty by helping workers to get salary without the inclusion of any transaction fee.

IX. APPLICATIONS OF BITCOIN

A. Tips and Donations

Bitcoin provides AN economical resolution for tips and contribution in many areas. sending a payment simply needs one click and receiving donations are often as easy as displaying a QR code. Donation are oftenvisible across the entire world, giving increased foil for non-profit governance. In cases of any emergencies, Bitcoin donations may contribute to a quicker International response.

B. Crowd Funding

Bitcoin proves useful in running Kick starter-like crowd funding campaigns, throughout which individuals pledge money to a project that is taken from them as long as enough pledges square measure received to satisfy the target. By processing these assured contracts by the Bitcoin protocol, helps in preventing a group action from happening until all conditions are met.

C. Micro Payments

Imagine listening to web radio paid by the second, viewing websites with a small tip for every ad not shown, or buying information measure from a wifi hotspot by the computer memory unit. Bit coin is adequate enough to make all of above ideas potential

D. Dispute Mediation

Bitcoin can be used to develop innovative dispute mediation services using multiple signatures. Such services could make it possible for a third party to approve or reject a transaction in case of disagreement between the other parties without having control on their money. Since these services would be compatible with any user and merchant using Bitcoin, this would likely lead to free competition and higher quality standards.

X. SMART CONTRACTS

Smart Contracts are self-fulfilling contracts, in line with the terms you set.

Smart contracts are also known as blockchain contracts and were introduced by a cryptographer and legal Scholar named Nick Szabo in 1994. It involves conversion of contracts to computer code, storing and replicating them. This would produce a ledger feedback like money transfer and receipt of service or product.

In the business scenario, small contracts automate how blockchain is used in the same way transactions of Bitcoins are carried out.

What Do Smart Contracts Provide You With?

- **Independence**

It is an independent system, which requires no middle person. It eliminates the use of middle person, lwyers, brokers. That's why, there is almost no potential risk of any third party manipulation due to the feature of automation .it improves the level of objectivity involved by eliminating potential bias and errors by individuals is completely.

- **Transparency**

Nobody can claim to have lost it because of the encryption of your documents on a common ledger, shared by the parties involved.

- **Secure**

The security provided in the websites are effectively very less . This is what known as cryptography. Your documents are ensured to be safe, as it would require an exceptionally intelligent hacker to get through the codes. Therefore it is ensured that your documents are not prone to hacking.

- **Savings**

With the deletion of middle or third party, intermediaries for that matter, smart contracts are proved to be a good way in saving your finances as you would need to hire a legal representative to check out as you make your transactions.

- **Accuracy**

There is considerable omission of errors when smart contracts are used. It is achieved due to the incorporated automation which help to bring about low costs and high speed, compared to completing many forms on a manual basis.

XI. INTERNET OF THINGS (IOT)

Internet of things (IoT), is one in all the foremost promising data and communication technologies (ICT), that is booming up within the to days world. IoT well integrate the things with web and provides users with numerous services. Some of the applications of IoT embody the provision management with Radio-Frequency Identification (RFID) technology, sensible homes, e- health, sensible grids, Maritime business (Wang et al., 2015), etc.[4]Blockchain technology is doubtless rising the IoT sector in some ways :-

- E-business propose a brand new IoT business model and notice the dealings of sensible property supported blockchai n and smart contract. during this model, distributed autonomous companies (DAC) is adopted as a suburbanized dealings entity. Individuals trade with DACs to get coins and exchange detector knowledge with none third-party.
- Safety and Privacy. Safety and privacy preservation is another vital concern Connected with IoT business. Blockchain facilitate in rising privacy in IoT applications. In

Particular to the present, Hardjono et al. (Hardjono and Smith, 2016) projected a privacy-preserving methodology, AN IoT device into a cloud scheme, it had been projected in (Hardjono and Smith, 2016) to assist device to prove its producing provenance without the authentication of third party and it's allowed to register anonymously.

REFERENCES

1. Pilkington, M ,Blockchain technology: principles and applications. Browser Download This Paper, 2015.
2. Atzori, M ,Blockchain technology and decentralized governance: Is the state still necessary?,2015.
3. https://www.finextra.com/blogposting/13068/5-ways-blockchain-will-transform-financial-services
4. Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain technology?—a systematic review. PloS one, 11(10), e0163477.
5. Mattila, J. (2016). The blockchain phenomenon–the disruptive potential of distributed consensus architectures (No. 38). The Research Institute of the Finnish Economy.
6. Ekblaw, A., Azaria, A., Halamka, J. D., & Lippman, A. (2016, August). A Case Study for Blockchain in Healthcare:"MedRec" prototype for electronic health records and medical research data. In Proceedings of IEEE open & big data conference (Vol. 13, p. 13).