# A Review Of Recent Blockchain Applications

Priteshkumar Prajapati, Krutarth Dave, Dr. Parth Shah

**Abstract**— Blockchain is considered a groundbreaking technology by many. It gives many features such as decentralization, persistence, anonymity, and transparency. Many researchers are trying to find out the maximum potential of blockchain. There is a wide range of blockchain applications such as cryptocurrency, financial and public services, healthcare domain, risk management, and so on. In this paper, recent applications proposed using blockchain are reviewed. The research domain contains healthcare, mobile security, smart contract security, cloud, and supply chain. This paper also reviews the precautions and security risks of using blockchain technology.

**Index Terms**— Blockchain, Cryptocurrencies, Smart Contracts, Blockchain Standards, Mining, Security, Privacy, Blockchain applications

## 1 INTRODUCTION

Blockchain became famous as an underlying technology of Bitcoin. It was first introduced in 2008 and it has gained a lot of popularity since then. At first it was used only for crypto currencies but then people realized that blockchain can be used for more than that. And now the application range of blockchain is very wide. Blockchain can be regarded as a public append only ledger, in which every transaction is stored in a block like structure. These blocks are connected with each other using cryptographic links. Every block is connected with its previous block. Every participant on the network holds the same copy of blockchain. That provides many benefits such as no single point of failure, equal rights of all participants, and detection of malicious activities. Every transaction in blockchain is done peer to peer. There is no intermediary involved. Participants who validate transactions and update the ledger are called miners. Miners compete to solve a difficult mathematical problem based on cryptographic hash functions and whoever wins gets to append the block. Miner who appends the valid block gets reward in terms of cryptocurrency. Many applications are there which can be made more efficient, secure and reduce the costs using blockchain. These application domains include healthcare, supply chains, government records, cloud, financial etc. As there are no intermediary involved for regulations, there are consensus mechanisms available to overcome that. Some of these consensus algorithms include proof-of-work, proof-of-stake, byzantine fault tolerance, and many more. One more feature that blockchain provided that of enabling use of smart contracts securely. Smart contract is a piece of code which is run automatically when certain conditions are met. These conditions are set prior the deploying the contract and with the signature of both the parties. So no party can deny of the terms they agreed upon. With the help of smart contracts, applications of blockchain sky rocketed. Many sectors implemented these smart contracts to avoid various kinds of problems.

## 2 LITERATURE SURVEY

### 2.1 INCEPTION OF BLOCKCHAIN

In [1], creators have given the introductory information about blockchain. The Blockchain first appeared from the paper “Bitcoin: a peer to peer electronic cash system” by Satoshi Nakamoto. Though paper was never submitted to a peer-reviewed journal. The problem Satoshi solved was that of the establishing trust in distributed systems. More clearly, the problem of creating distributed storage of timestamped documents where no party can temper with it without detection. And through digital signatures, it solved problems like authentication, integrity, and nonrepudiation. It doesn’t ensure the fraud-safe, but whenever it is happened, it gets detected and original values are established again. This can be achieved by recording every transaction in a ledger and on which every party has to trust. Blockchain contains the transaction timestamp, transaction details and hash of the current and previous block. Hash is a fixed length encrypted version of a string whose length doesn’t depend on string’s length. Blockchain is best known for the cryptocurrencies, but is not limited to. New applications are emerging to trade and specifically handle smart contracts, “Applications that run exactly as programmed without any possibility of downtime, censorship, fraud or any third party interference.” By the time, it will create many jobs never imagined because of the increasing trust of people in this technology.

### 2.2 BLOCKCHAIN STANDARDS

In [2], authors show the need of standardization for blockchain applications. In the past, to secure something, we used to isolate it from the external access to keep it safe. But blockchain is complete opposite of it providing independent verification rather than isolation. One of the key factors for success of distributed technology is that it can be easily added to existing system. Some people believe that blockchain will replace existing technology but in reality it will be add-on on current ones. There is much development with this technology going on. Cryptocurrency and record keeping are two main use cases of the blockchain. Many applications are now being created using blockchain. So there has been need for standardization for blockchain. And this standardization need to keep up with this emerging technology. The few of the targets are: Basic data models for blockchain, Consensus algorithms, Storage algorithms and web based access protocols etc. There has been few groups to deal with this too such as credentials community group, interledger community group etc. Hyperledger community is a great example of this. There are now more than 120 supporting industry members and a governance participation that allows for community participation. ISO TC 307 is now standards for blockchain and distributed technologies. This will be required to standardize the interoperability of different technologies with distributed ones.

### 2.3 BLOCKCHAIN APPLICABILITY

In [3], the team of author has investigated 23 blockchain projects in which they try to find that whether blockchain is the best fit for the problem or not. There are 10 things which we should consider before opting blockchain: Immutability, Transparency, Trust, Identity, Distribution, Workflow, Transactions, Historian record, Ecosystems, Inefficiency. Every aspect includes a series of questions to be asked before


- *Mr. Priteshkumar Prajapati, K.D. Patel Dept. of IT, CSPIT, CHARUSAT, Changa, Gujarat, India. E-mail: pritesh.pnp.007@gmail.com*
- *Mr. Krutarth Dave, K.D. Patel Dept. of IT, CSPIT, CHARUSAT, Changa, Gujarat, India. E-mail: krutarth.dave117@gmail.com*
- *Dr. Parth Shah from K.D. Patel Dept. of IT, CSPIT, CHARUSAT, Changa, Gujarat, India. E-mail: parthshah.ce@charusat.ac.in*

moving for next step. Such as for Trust, "Is there a need to establish or remove the need of trust? Is trust already established?", for Immutability, "Can database satisfy the need? What if mistake is made and correction is needed?" etc. At the end, there is one table given where the questions are written which are supposed to be asked before the project. In that we have to give score and then evaluate that by what %, we can be assure that blockchain is the solution for the problem. Out of 23 projects there were only 4 projects which can be sure that the blockchain is the solution. The main reasons for others not to pass were mainly because blockchain "was too costly for given economics", "was difficult to maintain sufficient distribution" and "encountered legal concerns that the ecosystem wasn't ready to accept".

### 2.4 BLOCKCHAIN COMPONENTS AND PROBLEMS

In [4], creators gives information about components, process and issues about blockchain. With the arrival of internet many data interchange are done online such as financial transactions for making payment or receiving. This entire transaction network is done through a trusted intermediary. This occurs questions about security that what if this party goes rough, what if data is lost, can't we go p2p etc. This is solved by blockchain where every participant has only a single copy of current ledger thus reducing the risk of single point failure and easing the detection fraud. There are 4 core components of blockchain: (1) Asymmetric key cryptography: doing transactions and managing wallet using public-private key, (2) Transactions: creating a block consisting of p2p transactions, (3) Consensus mechanisms: agreement of majority participants in network for a block, (4) Secured distributed ledger: a single copy of shared ledger. Block formation process in blockchain is divided into 2 phases. First is transaction generation and verification and second is consensus execution and block validation. There are 3 types of blockchain: public, private and consortium. Some of the consensus algorithms are: practical byzantine fault tolerance algorithm (PBFT- used by hyperledger), proof-of-work (used by bitcoin), and proof-of-stake [26] (used by Ethereum). Blockchain has many applications such as asset management, real estate, finance, IoT, Assisting wedding, health care and many more. Blockchain has some disadvantages like storage or scalability, high latency, fake block generation, energy consumption and has some risks such as 51% attack.

### 2.5 BLOCKCHAIN & CRYPTOCURRENCIES

In [5], the techniques for developing blockchain applications and gives some trending applications are given. Blockchain technology has potential to change the world even on economical level. As an example, the valuation of blockchain is more than the GDP of New Zealand country. That shows how big a blockchain application can be. There are 5 ways in which bitcoin is different from traditional cash or currency: (1) Bitcoin is completely decentralized, (2) Bitcoin is pseudo-anonymous, (3) Bitcoin has limited currency issuance, (4) Bitcoin is open-source, and (5) Bitcoin itself has no value, just a string of 0 and 1s. The cryptocurrencies other than bitcoin such as ether, ripple, bitcoin cash etc, are known as altcoins. There are mainly 6 dimensions of 6 different ways in which these altcoins are making progress. (1) Scalability: ex. Bitcoin cash (bitcoin fork That makes block size from 1 mb to 8 mb), (1) Privacy and security: ex. zcash, (2) Improving programmability of blockchain systems: ex. Ether, (3) Price stability: ex. USDT, (4) Innovation of consensus algorithm: ex. PeerCoin (5) Specific application oriented IOTA, Ripple. This paper proposes a 6 layer architecture for blockchain application. And the 6 layers are:

1. Data layer: includes data blocks, time stamp, hash functions, merkle tree and encryption.
2. Network layer: specifies the decentralized communication models and related mechanisms of distributed networking.
3. Consensus layer: different consensus algorithms such as PoX.
4. Incentive layer: incorporates economic rewards into blockchain community.
5. Contract layer: various smart contracts and algorithms are packaged and serve as a high level business logics to store data or asset on blockchain.
6. Application layer: contains all possible use case of blockchain

Here are 4 scenarios which are attracting investors and start-up companies: (1) Blockchain-powered smart contracts: blockchain when integrated with IOT and smart contracts can make automatic "smart property". 3 levels of intelligence (data, individual, social) may emerge in future. Data layer helps to keep a globally shared ledger. In individual layer, mobile devices and vehicles may become autonomous. In social level, robots can use these globally shared ledger for training purposes. (2) Decentralized sharing economy: platform like lazooz, a blockchain version of uber, can be the key element for sharing economy in future. (3) Blockchain-powered cargo transport: Many problems in shipping transport are there such as expensive operational cost, efficiency, data interoperability etc. blockchain can potentially solve these issues. Example of block-freight. (4) Blockchain based enterprise management and knowledge automation: blockchain can help in automating rules and regulations, can give tokens as incentive to employees etc.

### 2.6 TO BLOCKCHAIN OR NOT TO BLOCKCHAIN

In [6], the question that if we should use blockchain or not is discussed. The evolution of blockchain can be divided in to 3 parts. Blockchain 1.0, 2.0 and 3.0. 1.0 is for Bitcoin and cryptocurrency. 2.0 is for smart contracts applications such as registering, confirming, and transferring properties. In blockchain 3.0, it includes all sectors such as government, health, education and more. The general applications based on asset exchange includes financial transactions, public records, private records, intangible assets etc. There are number of prototypes available for different types of applications in fields such as personal data management, finance, trading, betting, government, commerce and supply chain, IOT etc. In this paper, a case study is provided for blockchain applications in insurance sector. There are 5 ways in which blockchain is envisioned to be applied: Using smart contracts to lower the operating costs and improve user experience, Fraud prevention, Data entry/identity verification, Pay-per-use insurance and Peer-to-peer insurance. To evaluate if blockchain should be used for these ways 5 questions are asked: "shared data need?", "multiple writers need?", "untrusted writers are there?", "disintermediation needed?", "linked transaction needed?" Among these

applications fraud prevention, data entry/identity verification, peer-to-peer insurance are the ones which are succeeded in all the categories. Other applications could apply the blockchain. But not so much need is there. So blockchain should not be seen as the “ultimate tech”, but rather should be used carefully after evaluating its impact and its need on the business.

### 2.7 DO YOU NEED A BLOCKCHAIN?

In [7], a different type of questionnaire is proposed before opting blockchain as a solution. Blockchain is an alternative way to remove the need of trusted third party form the architecture. And because of the replication of blockchain in peer to peer network, it is very difficult to change or corrupt the information. However, this feature alone is not enough to justify the use of blockchain in our application. There are numerous cases where blockchain should be avoided. In blockchain, removing of trust comes with a price in terms of speed. But in an application if you are okay to put the trust to one person or entity then there is no need of blockchain as it will be slower. There are a series of questions in a step wise manner that you must ask before opting the blockchain as a solution such as ‘Can a traditional database technology meet your needs?’ if no then, ‘Do you need more than one participant to update?’ if yes then , ‘do you need updaters to trust each other?’ etc. After all these questionnaire, you can decide what to opt. Public blockchain is not the only solution. Now blockchains can be built for private purposes. And transaction speed in private or permissioned blockchains is faster than public. If you want to show your activity to your participants but not the public, then you should go with the permissioned blockchain. Identity of every participant in permissioned network is known priory so that nothing shady can happen without being caught. So if the sacrifice of cost, speed and time is worth it, then only you should apply blockchain. But you should also consider that you might not need a blockchain.

### 2.8 MAKING SMART CONTRACTS SMARTER

In [8], a tool which uses symbolic execution to detect security flaws of the smart contracts is proposed. A smart contract is a program that runs on the blockchain and has its correct execution enforced by the consensus protocol. However, many vulnerabilities are there that can be exploited to cost so much money. These flaws arise because the semantic gap between the contracts is written and actual semantics. A smart contract is identified by a contract address. Each contract holds some amount of virtual coins (Ether), has its own private storage, and is associated with its predefined executable code. To invoke a contract at address users send a transaction to the contract address. There are many security bugs which should be handled while creating smart contracts. Some of them are:

1. Transaction-ordering dependence: when 2 transactions call the contract roughly at same time and order of the transaction effects the results.
2. Timestamp dependence: when changing the value of a timestamp can lead to miner-desired results.
3. Mishandled exceptions: when one contract is calling another but does not specifies or handle the returning values.
4. Re-entrancy vulnerability: while calling to another contract and waiting for another to finish.

To write better contracts for developers and avoid problematic contracts for users, a tool is proposed named “Oyente”. This analysis based tool is based on symbolic executions. It takes 2 inputs, one is bytecode of the contract and second is current Ethereum global state. And it answers the security problems contained by the contract. This tool is made using python and was tested against many smart contracts till around 1.5 million Ethereum blocks.

### 2.9 VERIFICATION OF SMART CONTRACTS

In [9], a framework to verify the smart contract security is given. Ethereum is a public blockchain which allows developers to develop a decentralized application in JavaScript-like language solidity. Since smart contracts are responsible for transfer of asset called “Ether”, security of smart contracts is very crucial. Solidity compiled code is converted into bytecode by EVM. When this code is deployed on Ethereum blockchain, it gives address to this contract. Though solidity provides classifiers, internal states of smart contract is public. Because of this, security concerns are important for any smart contract deployed. In this paper, a framework to validate the security of smart contract is suggested which translates contract to F*, a functional programming language which is aimed at program verification. This architecture uses 2 pronged approach. First one is solidity*, which compiles solidity contracts to F*. It verifies at source level, and check correctness of functions. Second is EVM*, it decompiles EVM bytecode into clearly expressed F* code. It allows to analyze low level code. The third part is checking the equivalence between solidity* and EVM* which is not discussed in this paper. This method uses shallow embedding and type-checking within existing verification framework.

### 2.10 BITCOIN MINING IS VULNERABLE

In [10], the threat on bitcoin mining is shown. Bitcoin’s security rests on distributive protocol which is maintained by participants and miners. To add transactions in the blockchain miner have to solve a puzzle. By solving a puzzle miner gets to attach the block to the chain and gain reward in terms of bitcoins. The more power the miner has, the better winning chances are. Miners form a mining pool in which they together solve the puzzle and is given reward according to the mining power he has given in solving the puzzle. There is one way that some miners can get more revenue than others, is called selfish mining. In selfish mining, when a selfish-pool finds a block, it keeps private. And tries to find next block. When honest miners, which follow the protocol correctly, reaches near to the lead of selfish miners, the pool publishes its private chain to the public which has more blocks than the chain which honest miners built. And as it is longest chain, it is accepted by the miners. And thus the work of honest miners is wasted and pool miners gets the reward. This paper shows that above a threshold size, revenue of selfish miners rises linearly. So a protocol modification is suggested which can lift up the threshold, thus requiring the higher pool size. When a miner gets 2 chains of same length, it propagates both of them instead of arbitrarily propagating one and choosing one branch randomly and trying to mine the block on that. Because of this, half of the honest miners will be working on the true

blockchain, and other half will be working on the selfish mining, thus reducing the risk of such selfish mining pools and increasing the threshold value.

### 2.11 BLOCKCHAIN WITH IOT

In [11], Blockchain with IoT is discussed. The reason blockchain is so popular is that it removes the need of intermediaries. It enables trustless system in a distributed manner. Current IoT ecosystem costs high for maintenance for manufacturers and has lack of trust for consumers. These problems can be solved using scalable, trustless peer-to-peer network which is transparent and distributed. Blockchain in IoT can be implemented in many ways. A manufacturer might update the firmware and set it in an IPFS system. When enough nodes has the update, the manufacture node can be stopped and saving the energy. Such way, smart contracts and its tokens can be used for renting cars or properties, energy sector, supply chain, etc. Using IoT with blockchain can hold disadvantages too. Transaction throughput will be low compared to centralized systems, maintaining privacy is hard as everything happens in open manner, it would be an assumption that miners follow the protocol honestly if many miners are not honest than its severe for transaction security, converting the tokens in real world money is not guaranteed are included. But creating failsafe mechanisms in network and smart contracts can impact at a large level while integrating IoT with blockchain.

### 2.12 SECURITY AND PRIVACY IN BLOCKCHAIN

In [12], authors survey on security and privacy of blockchain. Blockchain has grown a lot in recent years. Now there are hundreds of alter blockchains than Bitcoin. Some of them are similar to Bitcoin while many of them provide different functionality and security mechanisms. Distributed trust and security are 2 fundamentals for the blockchain technology. Here many paper's references are given which addresses many topics such as obstacles among distributed ledgers, correctness of smart contract, challenges for privacy on blockchain, suggestions for development and future threats.

### 2.13 BLOCKCHAIN IN DEVELOPING COUNTRIES

In [13], use cases in developing countries are given. Blockchain can be more useful to developing country than developed country. As it can help in keeping regulations, laws, rules etc. Property rights is one of the field in which many countries are struggling. Many fraud and abuse of government power are happening in property acquisition. 90 % of land is unregistered in rural Africa. It is common that government people alter the records of property and change the ownership to their own. With blockchain, these scenarios can be stopped. As every record is recorded in the chain, no one can escape that. In India, Andhra Pradesh and Telangana have accepted and taken the initiative to implement blockchain based property record system. Many countries are facing the issue of corruption in many fields. Cryptographically secured records make it much harder if not impossible to temper the data. We can create smart contracts to tag the properties such as cars, houses, metal containers or company shares too. So that every transaction attached with them can be stored. That helps in reduction of corruption. People who want to donate the people in need hesitate because the money many times does not reach to one who needs it. Blockchain can be a platform to enable that too. The money can directly be sent to the end party without the need of third party. For example, someone can directly pay the electricity bill of a person living in Africa with the help of Bitcoin or someone can pay directly the merchant for the food packages which can be then freely available to refugees.

### 2.14 AUTHENTICATED DATA FOR SMART CONTRACTS

In [14], authors targets the input quality of data feed to the smart contracts. Blockchain can be more useful to developing country than developed country. As it can help in keeping regulations, laws, rules etc. Property rights is one of the field in which many countries are struggling. Many fraud and abuse of government power are happening in property acquisition. 90 % of land is unregistered in rural Africa. It is common that government people alter the records of property and change the ownership to their own. With blockchain, these scenarios can be stopped. As every record is recorded in the chain, no one can escape that. In India, Andhra Pradesh and Telangana have accepted and taken the initiative to implement blockchain based property record system. Many countries are facing the issue of corruption in many fields. Cryptographically secured records make it much harder if not impossible to temper the data. We can create smart contracts to tag the properties such as cars, houses, metal containers or company shares too. So that every transaction attached with them can be stored. That helps in reduction of corruption. People who want to donate the people in need hesitate because the money many times does not reach to one who needs it. Blockchain can be a platform to enable that too. The money can directly be sent to the end party without the need of third party. For example, someone can directly pay the electricity bill of a person living in Africa with the help of Bitcoin or someone can pay directly the merchant for the food packages which can be then freely available to refugees.

### 2.15 A SOCIAL-NETWORK-BASED CRYPTOCURRENCY

In [15], a crypto-walled based system and its protocols are proposed. There are many cryptocurrency wallets are available in the market but the problem with them is they are mostly application oriented and not much secured. This paper proposes a semi-trusted social-network wallet system. It provides portable login on different device, login with no password authentication, blind wallet recovery and it is proven to be secure too. Unlike most crypto-wallets this system stores the identity link to device called "management device" so user doesn't need to remember long phrases to login. Management device is something that acts on behalf of used and stores encrypted user info on remote server. If user wants to perform transaction from any other device, it just needs to install proxy on that device. As it is a semi-trusted network, user can check the server's wallet but it can only read certain items in database. There are 5 protocols proposed for this system. Namely system setup, registration phase, master key backup, authenticated and wallet recovery.

### 2.16 ADAPTABLE BLOCKCHAIN-BASED SYSTEMS

In [16], a case study on product traceability is given. The authors have created an application called originChain, which provides transparent, temper proof traceability data, and automates regulatory-compliance checking. The problem is, all suppliers wants to receive the certificates to show consumers

the origin and quality of their product. And retailers also want those certificates to verify the quality and origin of the product. Traceability in originChain is flexible. As government regulations can be changed, and according to that, our code also changes, so this chain handles that dynamic change too. So, adaptability was the main concern for this. There are many steps to get the quality certificate such as getting lab results, getting verified from traceability service providers using paperwork. Every participant in the network, such as suppliers or retailers, are the node in the network and has the blockchain copy. After the producer gets verified by the TSP (Traceability Service Provider), originChain generates a smart contract which automatically checks if all the required details are provided or not, and it enforces conditions on which both the parties agreed. There are two types of storages: on-chain and off-chain. For privacy reasons, the personal details of the participants will not be shared on on-chain (like customer information). So this raw data is stored off-chain, but the hashes of those data is stored on chain. OriginChain stores 2 types of data on-chain, 1st hash of traceability certificate or photo, 2nd traceability information such as test results, origin, batch-number and inspection date. The raw files of the certificates are stored in MySQL database hosted by originChain. Every member of network can manage their own database. The generation of smart contract requires both TSP and suppliers authority. When the contract is generated, 2 contracts are created, registry contract and service contract. The registry contract represents the legal agreement and contains the address of service contract. The service contract can be modified by replacing the address of old address of service contract in registry contract by new address. The registry contract contains the list of address which are allowed to update the registry contract. If there are more than threshold authorities to agree on making change, then it'll be modified. To avoid any unauthorized access to the functions of code, smart contract also should have the control mechanisms which checks every time a function is called. Some challenges are also there, like lack of adaptability in suppliers of the new tech, efficient architecture, the cost of integrating blockchain etc. But even though blockchain provides a descent solution to the supply chain industry.

### 2.17 BLOCKCHAIN IN DUBAI GOVERNMENT

In [17], the projects run by Dubai government on blockchain are presented. Every government wants to reduce the time and complexity in paperwork and speed the delivery of services. Some experts believe that after shaking the financial industry, blockchain can make better the public sector too. 2 most early adopters are US state of Illinois and city of Dubai UAE. But there are some people who thinks otherwise. Robert Charette, an IT Risk management expert thinks that blockchain is just a solution to the problems which are already solved. Dubai is taking a path to build a single blockchain for every application. Every project will be launched on this single blockchain. And Dubai is planning to go paperless by 2020. Adapting blockchain fully on country level will definitely help the country in many ways. It will secure the records, speed up the process, save a lot of money, etc. According to smartdubai.ae, this will save 5.5 billion dirhams, cost of making one burj khalifa, per year. Illinois has a different approach. It will work on 5 different blockchains in different sectors. These 5 paths are, property titles, academic transcripts, vital records, energy market credits, and state licenses for health care providers. They are not concerned about how these blockchains will be integrated in future. They believe it will be solved by time when the technology matures.

### 2.18 BLOCKCHAIN IN HEALTH CARE

In [18], development of blockchain in health care domain is surveyed. Healthcare domain has some difficulties such as sharing historical records of the patient to other clinics. Because the patient takes treatment with many different doctors, and every doctor suggests different prescription, it is necessary to give all the past records to the clinic which you are visiting. Blockchain might be able to do that. It can keep the data secured as well as shared among the clinics and doctors. HIMSS (Healthcare Information and Management Systems Society) is trying to make do research for how blockchain will be able to transform today's medical records into e-records. Another is Blockchain Research Institute also doing research in many possible solutions which can be given using blockchain, and it is also publishing papers for how blockchain can be implemented in medical sector. Some researchers at MIT are also building a blockchain system called MEDRed, which allows user to give permission only to them whom he or she wants to see their data. It is a smart contract based application. There is another start up called patientory, which has been developing the blockchain for using in healthcare domain. It already has finished one pilot for gathering hospitals to make nodes to their network. This allows all the hospitals to share records among them. This follows top-down approach. Patientory has 3 tier architecture. First is presentation tier, which provides an application which connects users to the blockchain. Second is middle tier, where the off-chain computations are performed. And third one is blockchain, through which all data is transferred. Patientory has its own cryptocurrency named PTOY. It is used to buy extra storage to store the multiple records. There will be many hurdles such as hesitation of accepting new technology, gathering data, cost and complexity of development, etc. as we are at the beginning of new technological era. But many believes that this will be solved as the time goes.

### 2.19 BLOCKCHAIN IN LOGISTICS AND SUPPLY CHAIN

In [19], a method which can help in increasing the success ratio of developing successful application is proposed. Recently researchers are giving more focus to the various applications of blockchain such as supply chain. But the problem with these projects is lack of standard methodology for designing, developing and maintaining the application. Due to this many projects fail. Defining logistic network is a hard task as it involves many actors. Currently the challenge stays for the scalability or the number of transactions network can handle per second. Private or consortium blockchains have more scalability but it is more energy is wasted. To design application, GUEST method is used which can be used from idea to implementation. GUEST uses 5 steps, Go, Uniform, Evaluate, Solve and Test. At each stage of GUEST, we can monitor the progress or results and how to change them. There are 2 types of result from testing these on real applications. First is the blockchain solution for application, the solution is sustainable with the results and it saves many hours of optimization. The main advantage is the less waste of resources due to bad management. Second type of result is

for the methodology which allowed the transit from assessment of digital strategy to implementation in 4 months which took very less amount of time.

### 2.20 BLOCKCHAIN IN CONSUMER ELECTRONICS

In [20], blockchain applications on consumer electronics is surveyed. Although the primary use case of blockchain is cryptocurrencies, there are some use cases for Financial and Consumer Electronics sectors too. In this paper such articles are presented which shows blockchain use cases for Consumer Electronics, blockchain for health care, blockchain based smart cities and car insurance systems.

### 2.21 CLOUD/FOG SOLUTIONS USING BLOCKCHAIN

In [21], cloud solutions using blockchain are provided. Smart contracts and blockchain have the potential to change the current shape of cloud markets by enabling the development of completely decentralized cloud/fog solutions, which lower costs and enforce predictable results without requiring any intermediary. Current cloud offers are without any standards and is restricted to few providers. And every provider has its own vocabulary. Problems in current cloud can be solved by using a decentralized cloud system which also reduces the costs and predictable results for consumers without intermediaries.

Three projects are considered which are doing work in decentralizing the cloud with blockchain namely Golem, iExec and SONM. The common feature of all these three is that, due to high computational cost of mining, the smart contracts, transaction manager and reputation system are stored in separate chain called transaction network. And services are kept as off-chain called side chain. Golem is aimed to be a decentralized supercomputer. Golem provides SaaS service model. iExec is aimed to be a decentralized cloud. iExec provides all 3 service models SaaS, PaaS, IaaS. SONM is aimed to be a distributed fog supercomputer. SONM provides 2 service models, IaaS and PaaS. There are some challenges faced by these projects. They all rely on Ethereum and challenge for Ethereum is its scalability and it's per second transaction speed. The biggest challenge for these project is verification of the computations. Another challenges are the quality of service, checking the network performance in heterogeneous decentralized network and guarantee for data privacy. To avoid the incompatibilities among the projects such as QoS, service definition, execution workflows, management of components and identity and repudiation can be reduced using suggested standards.

### 2.22 BLOCKCHAIN ENABLED E-VOTING

In [22], a blockchain based e-voting system is proposed. The idea of e-voting is as follows. BEV (Blockchain E-Voting) issues a "wallet" containing user credentials. Each user gets a "coin" representing a single opportunity to vote. When the voter votes, the coin will be spent stopping them to vote more than once. Eligible voters cast a vote via computer or smartphone. BEV provides secure personal IDs. So no bad actor can engage in any activity. To hack the network, a hacker would have to hack most of the blocks before the new block enters the chain. Blockchain's ability to verify publically ensures that no one has voted wrongly or tempered any data. There are 2 start ups whose reference is taken here, Voatz and Agora. To see that how much voting is happening around the world, one example is, there were around 5000-7000 meetings were held in Moscow neighborhood. And these meetings have polls on different things. So many people needs voting systems to be secured. There are many benefits from this system. The vote is cryptographically secured record. So every vote is recorded accurate, permanently, securely and transparently. Many people can't attend meetings so they miss out the voting. But with this E-Voting, they can vote from their home. So it increases voting ratio. It costs less than the paper ballot system. There are many challenges too. Government and other stakeholders will be major challenge for e-voting. Although it provides security and privacy, public confidence and trust is also required. Every voter need to accept this technology as a trustworthy. The other challenge is immaturity of the blockchain. Also, blockchains require much more energy to perform authentication and so they are slow. So E-Voting using Blockchain is not yet to be used for national elections.

### 2.23 MALWARE DETECTION IN MOBILE DEVICES USING BLOCKCHAIN

In [23], a consortium blockchain framework is constructed to detect malware code and extracting it from mobile devices. It is composed of 2 chains, one consortium chain for testing members and one public chain shared by users. This method is particularly for android malware detection. There are 2 types of existing ways for malware detection, static and dynamic. Static used analysis of data flow in intermediate code but could not solve the encryption and other issues. That can be solved by dynamic by running stimulation of software. But still hackers can get past these. Result taking from a single feature doesn't give satisfactory results so here a corresponding multi-feature-model is built by adopting fuzzy comparison method to reduce false positives in result. A fact-base is also built to store the features detected from the malicious code.

The overall framework consists of 4 layers: network, storage, support and application. In network layer nodes communicate in p2p network. In storage layer the features of malicious codes are stored. In support layer the interface between users and fact base of malicious code. In applications layer interface and programs for different applications are provided. Features of android based software can be extracted from different features, such as package structure features, application and permission features, system call sequence features, and system call context features. After testing it, it gives more accuracy, lesser time than the previous methods.

### 2.24 EFFICIENT KEY MANAGEMENT FOR HEALTH USING BLOCKCHAIN

In [24], an effective method of key management for health blockchains is shown. Healthcare domain is one of the application domain of the blockchain. But it highly requires the data privacy and security. And privacy is mainly dependent on key management of the blockchain. With the help of new Body Sensor Networks, biosensor nodes can be deployed on/into human body and send the health reports of body to the nearby hospitals for further processing. If the data from this BSN goes in only one hospital, it creates many risks such as, single point failure, privacy issues and integrity issues. So we can migrate these data into the blockchain which has node in many hospitals avoiding above mentioned risks, by adding a gateway node with the sensors which send data to the blockchain. In addition, key is generated while adding data to the blockchain to maintain privacy. This paper shows the steps

to create keys and using them encrypt and decrypt the data. These are generated in such a way that attacking and retrieving keys or data are not possible with existing resources. The main advantage of this method is that this blockchain does not need to store encrypted keys but the clue of that key. The recovery of the key is executed by the BSN. That reduces the storage cost. The clue of encrypting keys is with the encrypted block, so the system does not need to search the related keys.

### 2.25 LIGHTWEIGHT WALLET BASED ON TRUSTZONE

In [25], a secure blockchain lightweight wallet is proposed. In bitcoin, instead of traditional username and password, there is high use of private keys. If you lost private key then the bitcoins are gone forever in the blockchain. That's why the security of private keys is essential. There are 2 ways to do transactions of bitcoin. One is software wallets which is easy to operate but less secure. And another is hardware wallet which is secure but have to be carried around. Most mobile devices do not have the memory to store the data of the blockchain on mobile, so Simplified Payment Verification (SPV) is popular now. Which can do transaction without storing the full block details but just the block headers. Then SPV connects to a full node in the network for the verification of transactions.

SBLWT is kind of in between. It is more secure than software based and it is more convenient than hardware based. Three objectives of SBLWT are confidentiality of private key, provide real and valid address, verification of transaction to be protected. SBLWT is based on TrustZone technology of arm. It also includes a touchscreen GUI for human-machine interaction. It is deployed on RASPBERRY PI 3 MODEL B board. For sake of security, there are 2 parts in the system, one is private (authentication data) and other is not so private (rich OS apps). It is designed for mobile devices so denial of service attack can be a threat for the application.

## 3 CONCLUSION

Blockchain is highly praised due to its advantages and offerings in the decentralized infrastructure. In this paper, the possible applications of blockchain in various fields are discussed. We also highlight the benefits and hurdles in these applications. This paper also reviews the security aspect of the blockchain and suggested changes. Blockchain has a lot of potentials with the benefits its offering but is still considered an immature technology. There has been so much work done and new features are introduced which increases usability and effectiveness of blockchain. But there are still many fields which still require more research and work so that these can be used as a practical solution. Example of these fields includes security, energy consumption, scalability, standardization, and transaction throughput.

## REFERENCES


[1] Di Pierro, Massimo. "What is the blockchain?." Computing in Science & Engineering 19, no. 5 (2017): 92-95.

[2] Anjum, Ashiq, Manu Sporny, and Alan Sill. "Blockchain standards for compliance and trust." *IEEE Cloud Computing* 4, no. 4 (2017): 84-90.

[3] Scriber, Brian A. "A Framework for Determining Blockchain Applicability." *IEEE Software* 35, no. 4 (2018): 70-77.

[4] Puthal, Deepak, Nisha Malik, Saraju P. Mohanty, Elias Kougianos, and Gautam Das. "Everything you wanted to know about the blockchain: Its promise, components, processes, and problems." *IEEE Consumer Electronics Magazine* 7, no. 4 (2018): 6-14.

[5] Yuan, Yong, and Fei-Yue Wang. "Blockchain and cryptocurrencies: Model, techniques, and applications." *IEEE Transactions on Systems, Man, and Cybernetics: Systems* 48, no. 9 (2018): 1421-1428.

[6] Gatteschi, Valentina, Fabrizio Lamberti, Claudio Demartini, Chiara Pranteda, and Víctor Santamaría. "To blockchain or not to blockchain: That is the question." *IT Professional* 20, no. 2 (2018): 62-74.

[7] Peck, Morgen E. "Blockchain world-Do you need a blockchain? This chart will tell you if the technology can solve your problem." *IEEE Spectrum* 54, no. 10 (2017): 38-60.

[8] Luu, Loi, Duc-Hiep Chu, Hrishi Olickel, Prateek Saxena, and Aquinas Hobor. "Making smart contracts smarter." In *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, pp. 254-269. ACM, 2016.

[9] Bhargavan, Karthikeyan, Antoine Delignat-Lavaud, Cédric Fournet, Anitha Gollamudi, Georges Gonthier, Nadim Kobeissi, Natalia Kulatova et al. "Formal verification of smart contracts: Short paper." In *Proceedings of the 2016 ACM Workshop on Programming Languages and Analysis for Security*, pp. 91-96. ACM, 2016.

[10] Eyal, Ittay, and Emin Gün Sirer. "Majority is not enough: Bitcoin mining is vulnerable." *Communications of the ACM* 61, no. 7 (2018): 95-102.

[11] Christidis, Konstantinos, and Michael Devetsikiotis. "Blockchains and smart contracts for the internet of things." *Ieee Access* 4 (2016): 2292-2303.

[12] Karame, Ghassan, and Srdjan Capkun. "Blockchain security and privacy." *IEEE Security & Privacy 16,* no. 4 (2018): 11-12.

[13] Kshetri, Nit, and Jeffrey Voas. "Blockchain in developing countries." *It Professional 20,* no. 2 (2018): 11-14.

[14] Zhang, Fan, Ethan Cecchetti, Kyle Croman, Ari Juels, and Elaine Shi. "Town crier: An authenticated data feed for smart contracts." In *Proceedings of the 2016 aCM sIGSAC conference on computer and communications security*, pp. 270-282. ACM, 2016.

[15] He, Shuangyu, Qianhong Wu, Xizhao Luo, Zhi Liang, Dawei Li, Hanwen Feng, Haibin Zheng, and Yanan Li. "A social-network-based cryptocurrency wallet-management scheme." *IEEE Access* 6 (2018): 7654-7663.

[16] Lu, Qinghua, and Xiwei Xu. "Adaptable blockchain-based systems: A case study for product traceability." *IEEE Software* 34, no. 6 (2017): 21-27.

[17] Nordrum, Amy. "Govern by blockchain dubai wants one platform to rule them all, while Illinois will try anything." *IEEE Spectrum* 54, no. 10 (2017): 54-55.

[18] Mertz, Leslie. "(Block) chain reaction: A blockchain revolution sweeps into health care, offering the possibility for a much-needed data solution." *IEEE pulse* 9, no. 3 (2018): 4-7.

[19] Perboli, Guido, Stefano Musso, and Mariangela Rosano. "Blockchain in logistics and supply chain: A lean approach for designing real-world use cases." *IEEE Access* 6 (2018): 62018-62028.

[20] Lee, Jong-Hyouk. "Blockchain Technologies: Blockchain Use Cases for Consumer Electronics." *IEEE Consumer Electronics Magazine* 7, no. 4 (2018): 53-54.

[21] Uriarte, Rafael Brundo, and Rocco De Nicola. "Blockchain-based decentralized cloud/fog solutions: Challenges, opportunities, and standards." *IEEE Communications Standards Magazine* 2, no. 3 (2018): 22-28.

[22] Kshetri, Nir, and Jeffrey Voas. "Blockchain-enabled e-voting." *IEEE Software* 35, no. 4 (2018): 95-99.

[23] Gu, Jingjing, Binglin Sun, Xiaojiang Du, Jun Wang, Yi Zhuang, and Ziwang Wang. "Consortium blockchain-based malware detection in mobile devices." *IEEE Access* 6 (2018): 12118-12128.

[24] Zhao, Huawei, Peidong Bai, Yun Peng, and Ruzhi Xu. "Efficient key management scheme for health blockchain." *CAAI Transactions on Intelligence Technology* 3, no. 2 (2018): 114-118.

[25] Dai, Weiqi, Jun Deng, Qinyuan Wang, Changze Cui, Deqing Zou, and Hai Jin. "SBLWT: A Secure Blockchain Lightweight Wallet Based on Trustzone." *IEEE Access* 6 (2018): 40638-40648.

[26] Sheth, Nakul, Priteshkumar Prajapati, Ayesha Shaikh, and Parth Shah. "Casper: Modification of Bitcoin Using Proof of Stake." In Information and Communication Technology for Intelligent Systems, pp. 79-85. Springer, Singapore, 2019.