PRIMARY, TECHNICAL AND IMPLEMENTATION BARRIERS IN BLOCKCHAIN TECHNOLOGY

Jyoti Yadav

Abstract—The first computing paradigm was the mainframe and personal computer, then the Internet revolutionized everything. Mobile and social networking was the most recent paradigm. The current emerging paradigm for this decade considered as one of the biggest technology breakthroughs is the connected world of computing relying on blockchain technology. Ever since blockchain technology came into existence it has been hogging a lot of limelight. The Blockchain was created to enable the first viable digital currency, known as Bitcoin. The idea was to have a decentralized currency that did not rely on banks or other financial institutions for its integrity or legitimacy. It is the technology upon which, most future business applications will be built and streamlined. It will be a novel method of data assemblage, data preservation and even trading. Here’s a look at why this vibrant and rather fascinating technology and its users might be posed with unique threats in the near future. This paper reviews the physical, technical and implementation barriers of blockchain technology and tries to understand the faults in the stars of blockchain.

Keywords—blockchain, distributed, Bitcoin, Ethereum, Hyperledger, cryptocurrency.

I. INTRODUCTION

Just as the Internet revolutionized the very idea of information, the latest buzzword, blockchain seems set to challenge and transform conventional notions of value. Technology’s success, however, depends on understanding its potential and applicability. Bitcoin, the cryptocurrency that pioneered blockchain technology is undergoing a riotous ride as financial regulators and governments start examining it in greater detail. However, the underlying blockchain technology has been picked up by practically every major technology and finance company. After all, it’s a ledger system that has an enormous potential to save infrastructure costs while providing secure and accurate transactions. Blockchain, needs to be examined closely for its misuse.

Blockchain is defined as a continuously growing lists of blocks that are linked and secured using cryptography. It is open, distributed ledger that records transaction details between two parties efficiently in a verifiable and permanent way. Blockchain is basically a persistent, transparent, public, append only ledger. It is a system that you can add data to without changing any previous data within it. The data added previously, remains intact. It does this through a mechanism for creating consensus scattered or distributed parties that do not need to trust each other, but trust the mechanism by which their consensus has arrived at. Blockchain attempts to solve 3 things:

1. To transfer money without the trusted middle party, for example a bank, thereby enabling people to connect directly with each other.
2. To transfer money faster than the traditional system. In fact, it would be transferred instantly or within a few minutes/seconds.
3. Making the costs of transferring cheaper than what the trusted middle party collects.

Every time you read about blockchain and how it works, one of the factors that jumps to the forefront is that the technology is dependent on a number of nodes that key in as well as save information at the same time. Each node/computer downloads the same information and saves it in
the same order. This means there is a lot of duplication and this duplicated data stays blocked in the 'chain' for posterity. A large network of individuals/nodes accept that a transaction made is true and is verified. Furthermore, all information about the said transaction will remain time stamped and tamper free on the chain that it is linked to.

Blockchain works on the fundamentals ideas of distributed, and open ledgers. Whenever a new block is added to the blockchain, it is shared with each node on the peer-to-peer network and every node verifies the authenticity of the block. They then arrive at a consensus, post which each node would add this block to their blockchain. Since it is decentralized, we can say that there is no central hub where the transaction data is stored. All details of the transaction in the blockchain is retained on the entire network, thereby ensuring the history is not in control of one person. This ensures complete security. In case of a conventional system, a trusted middle party ensures the authenticity of data, just like a centralized ledger. Therefore, we can say that blockchain allows for faster, safer and cheaper transfer of money as compared to conventional systems. Thus blockchain are remarkably transparent and decentralized way of recording lists of transactions.

II. LITERATURE REVIEW

Blockchain can be thought of as a comprehensive information technology with tiered technical levels and multiple classes of applications for any form of asset registry, inventory, and exchange, including every area of finance, economics, and money; hard assets (physical property, homes, cars); and intangible assets (votes, ideas, reputation, intention, health data, information, etc.). But the blockchain concept goes beyond this; it is a new shaping paradigm for the detection, evaluation, and transfer of all quanta of anything, and potentially for the coordination of all human activity at a much larger scale than has been possible before.

The research results of [1], investigate the positive implications of blockchain for modern organizations, specifically in the financial services industry or to manage physical asset ownership. However, the range of potential blockchain applications goes further to cover a multitude of business and social arrangements from tracking shipping containers and pharmaceuticals to recording gambling winnings and marriages based on smart contract embedded in blockchain applications.

A study by [2] adapts an established research framework to structure the insights blockchain technology, outline the present research scope as well as disregarded topics, and sketch out multidisciplinary research approaches. The framework differentiates three groups of activities (design and features, measurement and value, management and organization) at four levels of analysis (users and society, intermediaries, platforms, firms and industry). The review shows that research has predominantly focused on technological questions of design and features, while neglecting application, value creation, and governance. In order to foster substantial blockchain research that addresses meaningful questions, this study identifies several avenues for future studies. Given the breadth of open questions, it shows where research can benefit from multidisciplinary collaborations and presents data sources as starting points for empirical investigations.

The know-your-customer (KYC) due diligence process is outdated and generates costs of up to USD 500 million per year per bank. The authors of [3] propose a new system, based on distributed ledger technology (DLT) that reduces the costs of the core KYC verification process for financial institutions and improves the customer experience. In the proposed system, the core KYC verification process is only conducted once for each customer, regardless of the number of financial institutions with which that customer intends to work. Thanks to DLT, the result of the core KYC verification can be securely shared by customers with all the financial institutions that they intend to work with. This system allows for efficiency gains, cost reduction, improved customer experience, and increased transparency throughout the process of on boarding a customer.

In a paper by [4], the authors thoroughly review state-of-the-art blockchain-related applications. Reference [5] provides an initial step by showing: (i) the features and implementation challenges in healthcare interoperability, (ii) an end-to-end case study of a blockchain-based healthcare app we are developing, and (iii) how applying foundational software patterns can help
address common interoperability challenges faced by blockchain-based healthcare apps. In reference [6], the authors present a comprehensive survey on the state-of-the-art research efforts on blockchain technology particularly, giving an overview on blockchain technology. The typical blockchain consensus algorithms are then introduced. Next a survey on blockchain applications and technical challenges as well as recent advances is presented along with future research directions. Reference [7] presents a report on blockchain technology and its emerging opportunities and risks in detail in various application areas. The authors of [8] aim to analyse the current quality issues in blockchain implementation and to identify the blockchain quality attributes. A literature review is conducted to investigate the current quality requirements for blockchain implementations. Findings show that the research on quality requirements for blockchain is still in its early stage.

A systematic review of current research on blockchain technology has been conducted by [9]. The objective of the study had been to understand the current research topics, challenges and future directions regarding blockchain technology from the technical perspective by extracting 41 primary papers from scientific databases. The authors conclude that majority of the research in blockchain is focusing on revealing and improving limitations of blockchain from privacy and security perspectives, but many of the proposed solutions lack concrete evaluation on their effectiveness. Many other blockchain scalability related challenges including throughput and latency have been left unstudied.

In the paper by [10], the authors give an overview on blockchain research and development as well as introduce various research papers. They show that while blockchain has enabled bitcoin, the most successful digital currency, its widespread adoption in finance and other business sectors will lead to many business innovations as well as many research opportunities. The research goal of [11] is to understand whether the blockchain and peer-to-peer approaches can be employed to foster a decentralized and private-by-design Internet of Things (IoT). The authors gathered knowledge on the current use of blockchain technology and documented its current degree of integrity, anonymity and adaptability. Finally, a report on ‘how blockchain technology could change our lives’ by [12] conclude that blockchain technology is of increasing interest to citizens, businesses, government and organizations across the globe. The report also aims at providing a point of entry for those curious about blockchain technology, so as to simulate interest and provoke discussions around its potential impact.

III. A TECHNICAL PRIMER ON BLOCKCHAIN TECHNOLOGY

Blockchain presents a value proposition and provides a way to transact in a secure, immutable, transparent, and auditable way. However, the understanding of the technology varies widely in terms of its potential and applicability. This primer, thus aims to demystify blockchain and share the assessment of current and future scope, benefits and impediments, potential applications, and considerations for companies.

The potential benefits of the blockchain are beyond economic and extend into political, humanitarian, social, and scientific domains. In addition to economic and political benefits, the coordination, record keeping, and irrevocability of transactions using blockchain technology are features that could make blockchain technology popular. The blockchain can serve as warehouse for public records, including the archive of all documents, events, identities, and assets. Every asset to the blockchain can be encoded with a unique ID, such that the asset can be tracked, controlled, and exchanged (bought or sold) on the blockchain. This means that all types of tangible (houses, cars) and digital assets could be registered and transacted on the blockchain.

Blockchain technology has the potential to revolutionize financial transactions but there are several challenges to face in order to experience advantages. Blockchain has the capability to change the way we buy and sell, interact with government and verify the authenticity of everything from property titles to organic vegetables. It combines the openness of the internet with the security of cryptography to give everyone a faster, safer way to verify key information and establish trust.
heart, blockchain is a historical record of transactions, much like a database. Blocks in a chain is equal to pages in a book. Each page in a book contains:

The text: the story

Each page has information about itself like title of the book, chapter title, page text and page number.

Likewise, in a blockchain, blocks are a key part of the technology, and they have the following characteristics:
- They are small sets of transactions that have taken place within the system.
- Each new block includes a SHA-256 hash of the previous transaction that which “chains” it to all previous block.
- Blocks are computationally difficult to create, taking multiple specialized processors and significant amounts of time to generate.
- A header which contains the data about the block like technical information, a reference to the previous block, and a digital fingerprint or a hash of the data contained in this block, among other things. This hash is important for ordering and block validation.
- The contents of the block which is actually the information about the transaction(s).

The fact that blocks are both difficult to generate, and that in order to change one you’d have to successfully change all previous ones, makes the block chain particularly resistant to tampering.

3.1. Basic Idea of How Blockchain Works.

Blockchain is basically a chain or collection of blocks. Typically a block comprises of a **Header** which has different fields, a hash which is a cryptic value of **Previous Block** and **Transaction Details** in hashed form (Fig.1). The first block in the blockchain is known as **Genesis Block**. N number of transactions together make a block. These all block are distributed over the network as local copy on each connected node. The data that is stored inside the block, depends on the type of blockchain.

For example, a bitcoin blockchain stores the details about transactions like the sender, receiver and the amount of coins. A block also has a hash that identifies a block and all of its contents and it’s always unique, just like a fingerprint. Once a block is created, its hash is being computed. Changing the contents of the block will cause the hash to change. If the identity of the block changes, it is no longer the same block. The third element inside each block is the hash of the previous block. This creates a chain of blocks effectively and it is this technique that makes blockchain secure.

![Components of a Block](image)

**Figure 1. Overview of Blockchain Technology**
Once the maximum number of transactions in a block is reached, the three parts of the block which are header, transactions details & previous block hash are combined and hashed (encrypted) with a key known as proof-of-work or nonce. The correct key or proof of work is determined based on the difficulty level. For example we say a generated hash is valid if and only if it contains 5 leading zeros. So this leading 5 zeros is known as the difficulty level. The process of determining the right key is known as mining and it consumes the major time. Depending on which currency it is, rewards are given accordingly to the one who finds a valid proof-of-work. The moment someone finds a valid proof-of-work all the connected nodes are informed and if 50% of the nodes agreed then this new hash is added as a new block to the chain (Fig. 2).

| Block Structure | Block 1 | Process to get a Valid Hash |
|-----------------|--------|-----------------------------|
| Timestamp       | 201800303123030 | Keep on attaching NONCE incrementally in a loop to string of concatenated fields and generate the hash. This is repeated till a valid hash is found. |
| Index           | 0      |                             |
| Data            | N Transactions |                             |
| Prev Block Hash | 00000f43a5aae312 |                             |
| NONCE           | 1234   |                             |

Figure 2. Process to Get a Valid Hash

Where, the terms are defined as follows:

- **Block**: Group of transactions along with previous block hash and header data
- **Index**: Block number in the blockchain
- **Timestamp**: Time when block was generated
- **Prev Block Hash**: Hash of previously generated valid block
- **Difficulty**: The condition for verifying whether generated hash is valid or invalid, for eg. N number of leading 0’s
- **NONCE**: A number to find a valid hash
- **Merkle Tree**: Binary tree like arrangement of transactions in a block

### III. POTENTIAL APPLICATIONS OF BLOCKCHAIN

Blockchain can support a wide range of applications, and it’s already being used for peer-to-peer payment services, supply chain tracking and many more. The technology is still novel, but its potential is enormous. Here are some examples of how blockchain could hypothetically transform everyday transactions. Because blockchain establish trust, they provide a simple, paperless way to establish ownership of money, information and objects. The implications of blockchain technology in the financial services are far reaching and can potentially turn the entire industry down on its head.
The mammoth insurance sector known for its resilience to change is susceptible to high impact with the advent of blockchain technology. A Government, being the biggest and most influential service provider, can use the blockchain technology in a plethora of ways ushering in a new era of transparent and trusted governance. Organized supply chain management has been around since the fifties and blockchain could be the answer to solve its shortcomings. Probably the most crucial application of the technology, it has the potential to literally save lives is the healthcare sector. Internet of Things (IoT) is an up and coming avenue. It provides unthinkable possibilities for the future. However, it comes with its own share of problems and restrictions. The applications of blockchain could be categorised as follows:

**Financial Applications**
- Transactions
- Mortgage Services
- Commodity Exchange
- Remittances

**Non-Financial Applications**
- Government Service Applications
  - Audit Trait (Government Information)
  - Citizen Engagement Services
  - Identity Management
  - Intellectual Property
  - Land Transfers & Property Title Registrations
  - Management of Health Records
  - Vehicle Registrations
- Supply Chain Management Applications
- Technology Applications
  - IoT and Distributed Cloud

**IV. BARRIERS OF BLOCKCHAIN TECHNOLOGY**

Blockchain Technology suffers from many different types of drawbacks that include those related to technical issues with the underlying technology, ongoing industry thefts and scandals, public perception, government regulation, and the mainstream adoption of technology. Though blockchain is protected by high level of cryptography it isn’t 100% secure as it deals with large financial transaction attracting hackers. The primary, technical and implementation barriers discussed below could slow blockchain adoption.

4.1. Primary Barriers

Every new technology goes through the hype cycle that starts from its birth to its maturity and finally to its widespread usage and adoption. The primary barriers/obstacles to blockchain technology adoption are:

4.1.1 Regulations:

New products and services are evolving based on blockchain transactions, but there are currently no regulations on how the transactions should be written. Its distributed ledger transactions are likely to necessitate changes to industry regulations governing financial reporting as well as auditing processes.

Information-sharing regulations will likely need to be altered to protect companies as well as their investors and their customers. In addition, laws will need to be enacted that govern blockchains smart contracts.
4.1.2. Standards:
As with regulations, we currently lack one common set of standards for writing transactions on a blockchain. The regulations that evolve to regulate these standards will help drive the adoption of blockchain.

In short, the primary barriers to blockchain adoption is that since it is a promising technology, there are unknown factors or vulnerabilities that need to be looked upon.

4.2 Technical Barriers
A number of technical barriers related to the blockchain, have been identified and are in clear sight of developers, with different solutions to the challenges speculated. Some of these technical barriers include:

4.2.1 Throughput
It is the peak number of transactions/second. Blockchain technologies like bitcoin are currently unable to provide for more than 7 transactions per seconds (tps) and the transactions are recorded only once in every 10 minutes. VISA has a network strong enough to allow about 2600 tps. Twitter allows 15,000 tps at peak and advertising networks typically go beyond 100,000 tps. At the moment, the estimated number active blockchain users around the globe is around one in thousand. Linear increase in this number would result in a turmoil.

4.2.2 Latency
Block Latency is defined as the time required to add a block to the ledger and Consensus Latency is the time required to reach consensus on a new block. Right now, each bitcoin transaction block takes 10 minutes to process and get confirmed. For sufficient security, this time could be even more, about an hour or so as compared to VISA that takes seconds at the most.

4.2.3 Size
Each transaction or block added to the chain increases the size of the database. As every node has to maintain a chain to run, the computing requirements increase with each use. By having to download all the information on a blockchain every single time, individual nodes are pressed for capacity. Bitcoin, the largest company applying blockchain technology, currently has crossed 100 GB of system space. The latest smartphones or high configured laptops are going to get clogged with this size of data on it. Ethereum, a relatively new company that is revolutionizing the way smart contracts are built has already accumulated data of 200 GB in a much shorter life span.

The premise on which blockchain works is that everything that is linked on a blockchain is forever. All information is time-stamped and will remain in the system for future. There is an urgent need of increased access to system space, barring which the blockchain will not be able to reach its true potential. Inability to provide this extra space could mean risking already existing transactions on the blockchain too. In order to make money off the blockchain business, nodes have to download all the data on their chains. A lot of users realized that payments would not come through until all of the information had been downloaded to their computers indirectly involving a lot of time.

4.2.4 Wasteful
In order to maintain the consensus across the blockchain every node runs the blockchain giving extreme levels of fault tolerance, ensuring zero downtime, and making data stored on the blockchain forever unchangeable and censorship resistant. But this is all wasteful, as each node repeats a task to reach consensus burning electricity and time. This makes computation slower and more expensive than on a single computer.

4.2.5 Network speed/cost
Blockchain networks require nodes to run. But as many of the networks are new, they lack the number of nodes to facilitate widespread usage. Over time, successful public blockchain networks
will have to incentivize nodes, whilst creating favorable costs for users, with transactions completed in a relevant timeframe. This balance is key to the economics of each blockchain. Though the adoption of blockchain technology promises long-term benefits with regard to productivity, efficiency, timeliness and reduced costs, it is expensive to initially put it in place. The software required to run blockchain technology in organizations must typically be developed for the specific firm and is therefore expensive to purchase, acquire or develop in-house. Moreover, organizations may have to obtain specialized hardware for use with the software. This means that a move to a complete or even partial blockchain-based system is out of reach for most small- and medium-sized business due to the high setup costs involved.

4.2.6 Complexity

One of the biggest barriers between blockchain technology and the wider population is its complexity, and how difficult it is to understand and use for a layman. From hash rates, to address keys, orphan blocks, uncles and hard forks the blockchain world is full of concepts and processes that haven't been refined.

4.2.7 Limited scalability

Currently, all public blockchain consensus protocols have a challenging limitation: every fully participating node in the network is responsible for securing the system by processing every transaction and maintaining a copy of the entire state. While a decentralization consensus mechanism offers the core benefits of blockchain like—security guarantees, political neutrality, censorship resistance, etc.—it comes at the cost of scalability, since decentralization by definition limits the number of transactions the blockchain can process to the limitations of a single fully participating node in the network. Ethereum currently handles 800k transactions/day, while Bitcoin is nearing 500k. To address scalability issue a technique called sharding is used which would split the network up into smaller pieces called shards to improve transaction speed.

In other words, as the size of the blockchain grows, the requirements for storage, bandwidth, and compute power required by fully participating nodes in the network also increase. At some point, it becomes unwieldy enough that it’s only feasible for the few nodes that can afford the resources to process blocks leading to the risk of centralization.

4.2.8 Security and Privacy

Given that blockchain transactions are not tied directly to your identity, they may appear more private. Anyone in the world can create a new wallet anonymously and transact using it. Since this technology provides pseudonymity, transactions are recorded and stored in a public ledger, but they are linked to an account address that are comprised of alphanumeric characters. With no real-world identity attached to this address, the transaction’s originator seems impossible to track. However, this appearance of total security is misleading. It’s true that a person can preserve his or her privacy as long as the pseudonym is not linked to the individual, but as soon as somebody makes the connection, the secret is revealed. Thus the companies cannot upload critical business data into a blockchain where hackers, competitors, or other unauthorized parties can view the information. Consider the following examples of sensitive and confidential data:

- Electronic medical records cannot be made public on blockchains which may expose patient’s confidentiality.
- Identity verification data such as Aadhar Card numbers cannot be openly stored in a public smart contract.
- Credential management such as passwords and keys have no place in an open, ultimately unsecured smart contract.
- Financial documents such as employee salaries should never be publicly associated with addresses that are easily traceable.
Privacy remains a fundamental limitation for individuals, organizations, and industries that care about privacy and individual sovereignty. Many of us who are obsessed with blockchain and cryptocurrency have a determined interest in enabling a trustless and censorship resistant system that brings financial empowerment to the individual.

4.2.9 Lack of formal contract verification

Formal verification in relation to a software program is a methodology to determine whether the program behaves according to a specification. In general, this is done with a concrete specification language used to describe how the inputs and outputs of functions should relate. One example of a specification language is Isabelle, which is a generic proof assistant that allows mathematical formulas to be expressed in a formal language and provides tools for proving those formulas in a logical calculus. Another specification language is Coq, which is a formal language to write mathematical definitions, executable algorithms, and theorems. It is important to do formal verification for programs encoded within smart contracts as smart contracts are immutable, meaning they can’t be updated or fixed once they’ve been deployed onto the main Ethereum network. After deployment of the contracts they cannot be modified or updated.

Moreover, smart contracts are publicly accessible providing transparency but, it also makes smart contracts very attractive targets for hackers. Writing an error less smart contract is rather impossible. Moreover, with Ethereum, for example, verifying Ethereum Virtual Machine (EVM) code is incredibly difficult because of the way the EVM instructions are designed. This makes building formal verification solutions for Ethereum even more difficult. Regardless, formal verification is a strong approach to reducing the risk of bugs and attacks. They provide a higher guarantee of correctness than traditional approaches of testing.

4.2.10 Storage constraints

Most applications that get built on a public blockchain will require some sort of storage solution. However, storing information on a public blockchain database means that the data is:

- Stored by every full node in the network.
- Stored indefinitely since the blockchain database is append only and immutable.

Therefore, data storage imposes a huge cost on a decentralized network where every full node has to store more and more data into infinity. As a result, storage remains a huge hurdle for any realistic application that gets built on the blockchain.

4.2.11 Interoperability

Blockchain interoperability refers to the ability of the various blockchain systems to exchange information and make use of it. This has been a significant challenge in blockchain community since many developers create their own blockchains or blockchain-based applications in isolation from existing platforms. Moving value across chains always requires users to move their tokens to a centralized exchange, trade the assets, and then withdraw the converted asset onto the new chain of choice. This process is indeed time-consuming as well as expensive. Blockchains are currently isolated and unable to communicate with each other due to their decentralized nature, thus reducing scalability of each particular blockchain.

Very few of these blockchain platforms interact with each other, limiting their usefulness and increasing redundancy. One of the biggest driving factors focusing on the need for blockchain interoperability is the way that blockchains are verticalizing. Blockchains begin to verticalize, based on specific functions that they are performing thus creating their own sets of data and information that they record, in addition to the data analytics record. As each blockchain gets more information and works within itself, the question becomes how these various blockchains will communicate with each other. The Interoperability issue needs to focus on the common goal of connecting blockchain protocols.
4.2.12 Unsustainable consensus mechanisms

Users don’t have to trust anyone else with their transactions on blockchain thus achieving autonomy, censorship resistance, and authenticity.

a. Proof-of-work consensus

Proof-of-work is a protocol that consists of solving problems that are difficult to solve, but easy to verify. The issues with proof-of-work are that they require specialized hardware, large memory and high bandwidth, mining pool centralization that mines the pool, and energy consumption in terms of electricity and computation costs.

b. Proof-of-stake consensus

Proof-of-stake eliminates the need for hardware and is inherently more energy efficient than proof-of-work. Proof-of-stake algorithms have their own fundamental challenges.

4.3 Implementation Barriers

Implementation of blockchain technology involves three things: blockchain ledger, blockchain network and blockchain clients. Security, privacy, throughput, size and bandwidth, performance, usability, data integrity and scalability are some of the attributes required for high quality blockchain implementation.

4.3.1 Integration with Legacy Systems

In order to make the move to a blockchain-based system, an organization must either completely renovate their previous system or find a way to integrate their existing system with the blockchain solution. However, it may be difficult for blockchain solutions to handle all functions needed by organizations, initially making it difficult to completely eradicate legacy systems. Therefore, considerable changes must be made to the existing systems in order to facilitate a smooth transition. This process may take a significant amount of time, funds and human expertise. In some cases, it may be undoable to reconcile the two systems, and the organizations must acquire new systems that are compatible with the blockchain solution. Many organizations are reluctant to make the move to blockchain solutions because of time and money that would be required in order to achieve successful company-wide implementation.

4.3.2 Energy Consumption

The Bitcoin and Ethereum network both use the proof-of-work mechanism to validate transactions made on the blockchains. This mechanism requires the computation of complex mathematical problems to verify and process transactions and to secure the network. These calculations require large amounts of energy to power the computers solving the problems. In addition to the energy used to run the computers, a sizable amount of energy is also required to cool down the computers. With climate change being a major concern, such massive use of energy does not seem justifiable. Use of proof-of-stake mechanism would be more sensible with regard to energy consumption.

4.3.3 Public Perception

Majority of the public is still unaware of the existence and potential uses of blockchain technology. Though the technology is revolutionizing many different industries, knowledge of the benefits of distributed ledger technology is still limited to those who are involved in the technology space and those whose industries are adopting blockchain solutions. People should understand the difference between different cryptocurrencies and the blockchain which may help in increasing the willingness to use the technology.

4.3.4 Planning of the Blockchain Project

It is more expensive and time consuming to build a blockchain application than a traditional cloud application in many situations.
4.3.5 Deciding the Technology

Two popular platforms of technology that can be used are: with a Crypto Currency (Ethereum) and without a Crypto Currency (Hyper-Ledger Fabric). The technology along with its standards has to be decided depending on the problem at hand. Ethereum Wallet allows users to hold and secure ether and other crypto-assets built on the Ethereum blockchain platform, as well as write, deploy and use smart contracts. Hyperledger is an open source global collaboration hosted by The Linux Foundation to advance cross-industry blockchain technologies. Some of the business blockchain frameworks hosted with Hyperledger are:

- Hyperledger Fabric: Blockchain technology implementation intended to facilitate development of blockchain applications or solutions.
- Hyperledger Iroha: Distributed ledger for simple and easy incorporation into infrastructural projects.

4.3.6 Requirement of Blockchain Developers

There is a need to have experienced blockchain developers and architects on the team to guide a project to fulfilment.

4.3.7 System Support Services

For enterprises, simply building the application is not sufficient. Applications need to be deployed into production and supported. Developer support includes; i) curated knowledge bases for blockchain technology, core components and developer tools ii) community support through forums iii) live support from technical support engineers including break fix.

4.3.8 Infrastructure

This includes building industry standard, open source, free-to-use blockchain solutions that will be the foundation for future businesses. Legal aspects of blockchains and smart contracts, industry areas such as banking and supply chain, and of course core technology issues such as privacy, permissioning and networking standards have to looked upon.

4.3.9 Blockchain Stack and Tools

The developers need to have knowledge about blockchain stack and the emerging tools that can be integrated into existing development environments and frameworks, such as continuous integration, testing frameworks, automated deployment and dev-ops.

4.4 Mining Issues

Blockchain brings with it the concept of mining. Miners will usually have entire computer systems that are dedicated to a singular task-mining cryptocurrency. Their job is to create new blocks in a blockchain. The current payout for creating a new block for Bitcoin is 12.5 bit coins. This payment by June 2020 will be halve when 210,000 blocks are added.

Miners have to burn a lot of electricity to make this work. Not every block gets instant approval to be added at the end of a chain. The miners work hard to make a block ‘beautiful’ before it can be approved to reach monetary potential for its creator. Given that new blocks cannot be added more than once in 10 minutes to avoid transaction rewriting, a lot of energy is consumed in that wait time by n number of miners trying to shake down blocks to create one beautiful one ! The cost of specialized mining equipment gets added to energy consumed.

4.5 Risk of External Attacks

Blockchain is based on a large network of nodes. Each of these nodes have the same information stored in them. This would mean that the information, even if wiped out from one server would stay safeguarded because it has so many other redundant copies. The nodes are thus susceptible to external attacks. Gaining control over computers from 4 to 5 top mining groups could
give a terror group the chance of carrying out a majority attack on the miners and blockchains of the world.

4.6 Financial Transparency is a problem

Blockchains are popular for anonymity and financial transparencies. Digital money is used to purchase almost every commodity. The issue with financial transparency would be lack of privacy. While this kind of transparency is more of a cosmetic problem for individuals, the repercussions it has on the ledgers of larger companies is very real. They could be sending out information with regards to tenders and other such sensitive data to anyone linked to their blockchains. While private blockchains seems to have solutions for these issues, a public blockchain like Bitcoin is not very useful for companies with big bank balances and multiple financial transactions.

V. CONCLUSIONS

Blockchain Technology is a framework for decentralizing a number of entities that required a middlemen and involve significant opacity. Blockchain could be a revolution in the way businesses, government, organizations and individuals work together. It provides a simple, secure way to establish trust for virtually any kind of transaction, helping simplify the movement of money, products or sensitive information worldwide.

For the technology to be implemented, there is an immediate need for effective laws that cater specifically to it. People need to be educated about blockchains and how it can help them and change the way they do business or even everyday transactions. To fully benefit from blockchains enormous potential, enterprises must first overcome two formidable challenges: standardization and interoperability. Robust solutions that are capable of inter-blockchain communication to allow multiple chains to communicate and transact with one another flawlessly need to be looked out. More efficient signature schemes and other cryptographic systems that low-resource devices can handle without sacrificing security should be thought of.

REFERENCES

[1] R. Beck, M. Avital, M. Rossi, and J. B. Thatcher, “Blockchain Technology in Business and Information Systems Research,” Business & Information Systems Engineering: The International Journal of WIRTSCHAFTSINFORMATIK, vol. 59(6), pp.381-384, 2017.
[2] M. Risius and K. Spohrer, “A Blockchain Research Framework,” Business & Information Systems Engineering, vol. 59(6), pp. 385-409, 2017.
[3] J. P. Moyano and O. Ross, “KYC Optimization using Distributed Ledger Technology,” Business & Information Systems Engineering, vol. 59(6), pp. 411-423, 2017.
[4] B. A. Tama, B. J. Kweca, Y. Park, K. H. Rhee, "A Critical Review of Blockchain and its Current Applications,” International conference on Electrical Engineering and Computer Science (ICECOS), IEEE, pp. 109-113, 2017.
[5] P. Zhang, J. White, D. C. Schmidt, G. Lenz, "Applying Software Patterns to Address Interoperability in Blockchain-based Healthcare Apps," arXiv preprint arXiv:1706.03700. Jun. 2017.
[6] Z. Zheng, S. Xie, H. N. Dai and H. Wang, “Blockchain Challenges and Opportunities: A Survey,” Work Pap., 2016.
[7] Sorell, W.H., General, A. and General, V.O.A., 2016. Blockchain Technology: Opportunities and Risks. Vermont Office of the Attorney General.
[8] B. Koteska, E. Karafilovski and A. Mishev, “Blockchain Implementation Quality Challenges: A Literature Review, Proceedings of the SQAMIA: 6th Workshop of Software Quality,” Analysis, Monitoring, Improvement, and Applications, Belgrade, Serbia, pp.11-13, 2017.
[9] J. Yli-Huumo, D. Ko, S. Choi, S. Park and K. Smolander,"Where is Current Research on Blockchain Technology?—A Systematic Review.,” PloS one, vol. 11(10), p.e0163477, 2016.
[10] J. L. Zhao, S. Fan and J. Yan, “Overview of Business Innovations and Research Opportunities in Blockchain and Introduction to the Special Issue,”2016.
[11] M. Conoscenti, A. Vetro and J. C. De Martin, “Blockchain for the Internet of Things: A Systematic Literature Review,” In Computer Systems and Applications (AICCSA), IEEE/ACS 13th International Conference of IEEE, pp. 1-6, 2016.
[12] P. Boucher, “How Blockchain Technology Could Change Our Lives: In-depth Analysis,” European Parliament,2017.