TITLE:BLOCK CHAIN FROM A DISTIBUTED COMPUTING PRESPECTIVE

NAME:K.NITHIN REDDY
ROLL NO:15E11A05F0
BRANCH:CSE
SECTION:C

1.INTODUCTION

1.1 BLOCK CHAIN AS A TRANSACTION:

Blockchains are tamper evident and tamper resistant digital ledgers implemented in a distributed fashion (i.e., without a central repository)and usually without a central authority (i.e., a bank, company or government). At their basic level, they enable a community of users to record transactions in a shared ledger within that community, such that under normal operation of the blockchain network no transaction can be changed once published. In 2008, the blockchain idea was combined with several other technologies and computing concepts to create modern cryptocurrencies: electronic cash protected through cryptographic mechanisms instead of a central repository or authority.

This technology became widely known in 2009 with the launch of the Bitcoin network, the first of many modern cryptocurrencies. In Bitcoin, and similar systems, the transfer of digital information that represents electronic cash takes place in a distributed system. Bitcoin users can digitally sign and transfer their rights to that information to another user and the Bitcoin blockchain records this transfer publicly, allowing all participants of the network to independently verify the validity of the transactions. The Bitcoin blockchain is independently maintained and managed by a distributed group of participants. This, along with cryptographic mechanisms, makes the blockchain resilient to attempts to alter the ledger later (modifying blocks or forging transactions). Blockchain technology has enabled the development of many cryptocurrency systems such as Bitcoin and Ethereum1. Because of this, blockchain technology is often viewed as bound to Bitcoin or possibly cryptocurrency solutions in general. However, the technology is available for a broader variety of applications and is being investigated for a variety of sectors.

The numerous components of blockchain technology along with its reliance on cryptographic primitives and distributed systems can make it challenging to understand. However, each component can be described simply and used as a building block to understand the larger complex system. Blockchains can be informally defined as: Blockchains are distributed digital ledgers of cryptographically signed transactions that are grouped into blocks. Each block is cryptographically linked to the previous one (making it tamper evident) after validation and undergoing a consensus decision. As new blocks are added, older blocks become more difficult to modify (creating tamper resistance). New blocks are replicated across copies of the ledger within the network, and any conflicts are resolved automatically using established rules.

The theory of decentralized crypto-currencies (e.g. Bitcoin and Altcoins) have gained rapidly recognition and are often associated with statements such as a glimpse into our future . While the Bitcoin technology has been extensively studied, we believe that the concept of the Blockchain provides a new perspective on the already existing literature by looking at the various appliances of the underlying technology in a socio-economical setting prior to its previous literary focus within finance and economics (e.g. fin-tech). While Blockchain represents a novel application on cryptography and information technology, researchers still lack to find the tipping point for the technology. Researchers agree that the Blockchain technology has certain features that is well applied within the financial industry , but still lacks Preprint submitted to Mannheim University, 7th November 2017 January 9, 2018 to find the appropriate use of large scale Blockchain usage within modern society . This is further backed by researchers that points to the fact, that crypto currencies and Blockchain has not yet reached mainstream IS research. However, technologies such as automation, computing, robots and ultimately the Internet have been contributing immensely to progression and wealth of economies and cultures and thus expect that the Blockchain technology will provide further contributions.

1.2 MOTIVATION:

The goal of this paper is to summarise the literature on implementation of the Blockchain and similar digital ledger techniques in various other domains beyond its application to crypto-currency and to draw appropriate conclusions. Blockchain being relatively a new technology, a representative sample of research is presented, spanning over the last ten years, starting from the early work in this field. Different types of usage of Blockchain and other digital ledger techniques, their challenges, applications, security and privacy issues were investigated. Identifying the most propitious direction for future use of Blockchain beyond crypto-currency is the main focus of the review study. Blockchain (BC), the technology behind Bitcoin crypto-currency system, is considered to be essential for forming the backbone for ensuring enhanced security and privacy for various applications in many other domains including the Internet of Things (IoT) eco-system. International research is currently being conducted in both academia and industry applying Blockchain in varied domains.

The Proof-of-Work (PoW) mathematical challenge ensures BC security by maintaining a digital ledger of transactions that is considered to be unalterable. Furthermore, BC uses a changeable Public Key (PK) to record the users' identity that provides an extra layer of privacy. The successful adoption of BC has been implemented in diverse non-monetary systems such as in online voting, decentralized messaging, distributed cloud storage systems, proof-of-location, healthcare and so forth. Recent research articles and projects/applications were surveyed to ascertain the implementation of BC for enhanced security and to identify its associated challenges and thence to propose solutions for BC enabled enhanced security systems. The knowledge domain of the research is in the realm of the digital ledger, specifically, in Blockchain and crypto-currency.

2.INDUSTRIAL APPLICATIONS AND DISCUSSIONS

2.1 ORIGIN OF BLOCKCHAIN TECHNOLOGY:

The paper utilizes a combination of the approaches identified by Brocke et al., Webster and Watson and Meller-Bloch and Kranz. The combination of these literature review- frameworks will ensure both the rigor of the research contributions of this paper. The frameworks will also ensure the reproducibility of the results and conclusions drawn. We will use the framework by Brocke et al., that consists of five phases; In phase one, the scope of the review needs to be determined. In phase two, the topic of the paper should be conceptualized which includes creating definitions for the key terms. Third, the literature search needs to be conducted. In the fourth step, the literature is analyzed and synthesized. Finally, in the last phase, we establish the research agenda, Thus, the identification of research gaps is included in the last step (Phase V) of Brocke et al.s framework.

- **Scope:**

According to Bacharach and Whetten , it is important to define the boundaries of a paper, including the scope. This paper focuses on the main IS contributions within the largest academic journals (AIS, IEEE, EJIS, MISQ etc.) and within the majority of IS conferences (ECIS, ICIS etc.). However, we will also look at the general research contribution on e.g. Google Scholar to establish a general baseline of the topic to identify all relevant literature, due to the novelty of the technology. With the identification of relevant literature, we will analyze and synthesize the results found in the literature in order to identify gaps and propose frameworks for future research. Lastly, a conclusion will be established to provide researchers with the main contributions of the paper. However, in this paper, we will exclude the technological aspects of the technology, as previous research already has focused on aspects of the technological infrastructure in terms of security, anonymity, scalability e.g. [6, 7, 8]. Lastly, we will also exclude the economic use cases of the technology (e.g. Bitcoin) and focus solely on the technology behind, the Blockchain.

• Topic conceptualization:

The main concept of this paper is focalized around the Blockchain technology, which we previously defined as a ”[...] shared digital ledger”. Based on the Blockchain, we will take a deeper look into two sub concepts; platforms and ecosystems to establish a common point of reference for our literature review. With this setting, we will look at how the current and previous literature describes the Blockchain in a platform and ecosystems context. Hence, our main search will be aimed at finding literature that describes the Blockchain as an enabler for ecosystems, or the Blockchain as a future platform in mainstream research. Accordingly, we have chosen the keywords; Blockchain and Ecosystems for our literature search.

• Literature search

Brocke et al. describes the third phase as the literature search. In this phase we explain the methodological framework for conducting the literature search. According to Webster and Watson and Brock et al., the search can be conducted in different ways. Webster and Watson suggest starting the search for relevant literature in leading journals. However, the literature search in this paper was divided into four phases. First, we establish a common ground by searching generally for the concepts across various platforms to identify a knowledge base as the foundation for the literature review. As established above, the primary focus has been on the keyword Blockchain, due to the fact that extensive literature exists on both ecosystems and platforms. Second, when the common ground has been established, we identify the primary drivers within the IS research field. We take foundation in the senior scholar’s basket of journals, in which we identify the basket of eight, consisting of the essential journals within IS research. However, there exist various ways of identifying literature with high quality. Additionally, we also identify other relevant journals, that is included in our database search. In step three, we conduct a forward and backward search to ensure that we have exhausted the concepts within the area of interest.

The literature found in step three is mapped into a customized version of Brocke-etal.s backward/forward matrix. After we conclude that we have reached an exhaustive point of our research, we add the literature found in the forward/backward search to our original concept matrix to ensure a full overview of the topic. However, we note that due to the exclusion of technical papers, we cannot claim to be exhaustive, but note that we reach a point of theoretical saturation with the selected articles. Theoretical saturation is reached, when no new categories and properties emerge from the data .During our general search, we start out by searching for literature on Google Scholar to create a quick overview of the research topic. During this phase, we use a concept matrix approach [10, 23], where the concepts are identified and mapped in the matrix. This allows us to get a full overview of the research landscape within our topic of interest. After an overview has been established, we follow the guidelines by Brocke et al. by following a rigor search process by searching the main contributing journals within the IS field. However, as the topic is still considered novel, we also consider the main conference publications within IS to ensure that the topic has been exhaustively examined.

With the identification of the main contributing journals and conferences, we establish our journal overview by creating a database matrix to identify journals, databases, search, coverage, hits and literature reviewed (appendix B). We map the found literature into our concept matrix. When all the identified journals and conferences has been searched, we continue to the next phase where we conduct a forward and backward search on all the found literature in the general search. As mentioned previously, we utilize a customized version of the framework by Brocke-etal. , in which we map each of the papers based on the following parameters; Number of article references, number of articles citing the original article, period covered, keywords, relevant backward search papers and lastly, relevant forwards search papers. We furthermore divide both forward and backward papers into two categories; new and existing literature. Thus, with this customized matrix we get a quantitative overview of all the papers covered in the literature review.

2.2 OBJECTIVE :

This document provides a high-level technical overview of blockchain technology. It looks at different categories of implementation approaches. It discusses the components of blockchain technology and provides diagrams and examples when possible. It discusses, at a high-level, some consensus models used in blockchain networks. It also provides an overview of how blockchain technology changes (known as forking) affect the blockchain network. It provides details on how blockchain technology was extended beyond attestable transactions to include attestable application processes known as smart contracts. It also touches on some of the limitations and misconceptions surrounding the technology. Finally, this document presents several areas that organizations should consider when investigating blockchain technology. It is intended to help readers to understand the technologies which comprise blockchainnetworks.

The goal of this paper is to conduct a literature review of the current literary landscape within the field of IS. We will look at the Blockchain technology, and analyse prior literature in order to identify gaps in the current literature. Motivated by its technical and mathematical nature, previous research has focused exclusively on aspects of the technological infrastructure such as security, anonymity, scalability or the resiliency of consensus mechanisms. Due to the novelty of concepts and the underlying technologies, we provide a new overview on recent developments and related literature in this paper and strive to explore the related concepts in the literature.

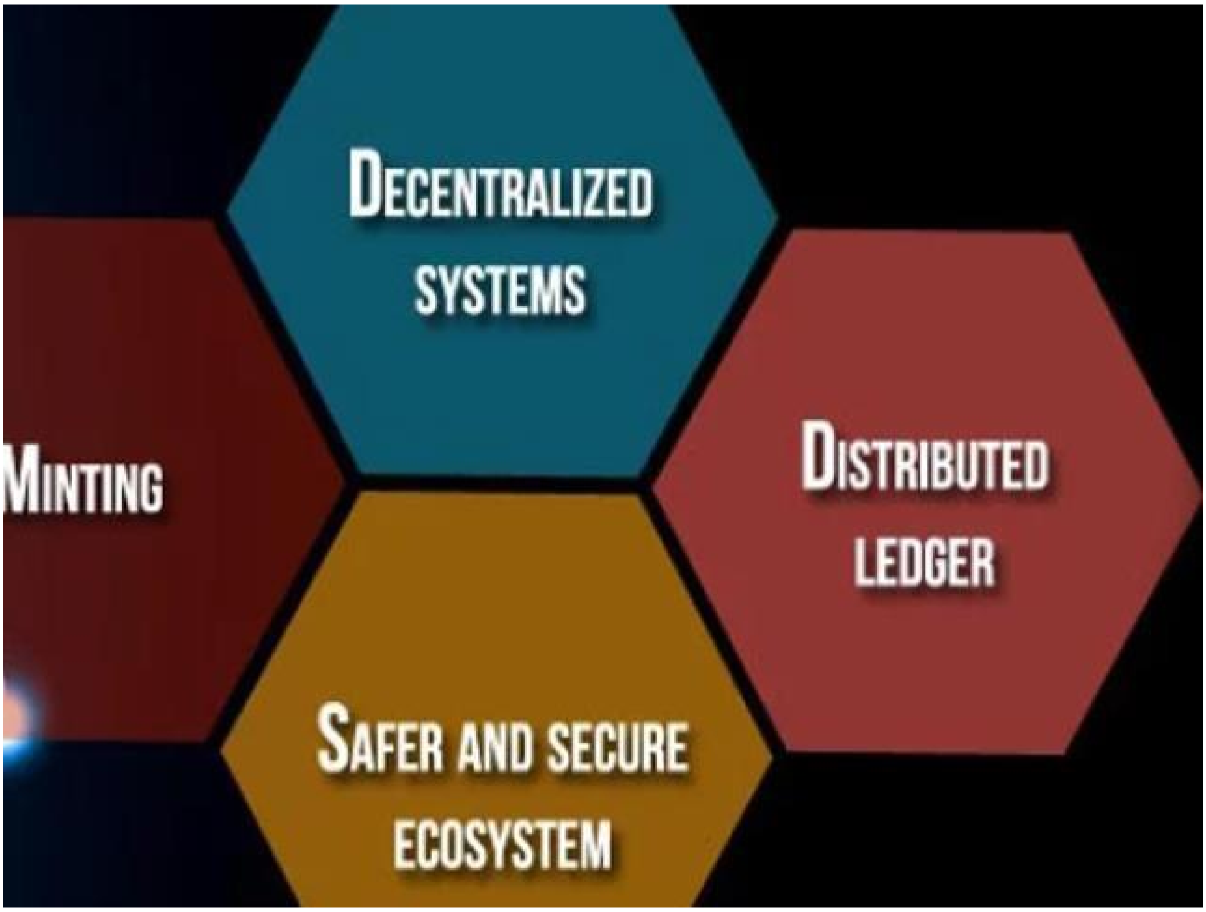
Through exploration of the concepts, we dive into the Blockchains utilization as a technological platform for an upcoming ecosystem of applications and software and look at the theoretical features of the technology as a foundation for this paper. Thus, we seek to enhance the understanding of the technology in other contexts throughout the literature and explore the current contributions to the literature. This study has implications for both researchers and practitioners. For researchers we seek to identify a new branch of research that focuses on enablement of the Blockchain as a platform-centric technology for ecosystems to flourish.

For practitioners, we illustrate that it is crucial to keep developing on the technology, as research indicates that we have still not reached the tipping point of the technology. Hence, this paper aims to answer the following research questions:

- Is the Blockchain technology able to establish itself as a mainstream platform for ecosystems based on its current capabilities?

- Does the Blockchain provide enough technical capabilities to be considered a sustainable platform and reach mainstream adoption?

  - To gain a basic knowledge about the Cryptocurrencies.
  - To study the advantages and Disadvantages of Cryptocurrencies.
  - To study the present scenario of Cryptocurrencies worldwide.
  - To Study the future scenario of Cryptocurrencies.



2.3 TOPIC DESCRIPTION :

Blockchain technology can seem complex; however, it can be simplified by examining each component individually. At a high level, blockchain technology utilizes well-known computer science mechanisms and cryptographic primitives (cryptographic hash functions, digital signatures, asymmetric-key cryptography) mixed with record keeping concepts (such as append only ledgers). This section discusses each individual main component: cryptographic hash functions, transactions, asymmetric-key cryptography, addresses, ledgers, blocks, and how blocks are chained together. Blockchain is the technology behind Bitcoin. A block is a collection of all the recent transactions that have happened and verified. In simple terms, the technology handles blocks uniquely identified, linked transaction records in a chain. A blockchain is a continuously growing, distributed, shared ledger of such blocks, which are sealed cryptographically with a digital fingerprint generated by a hashing function.

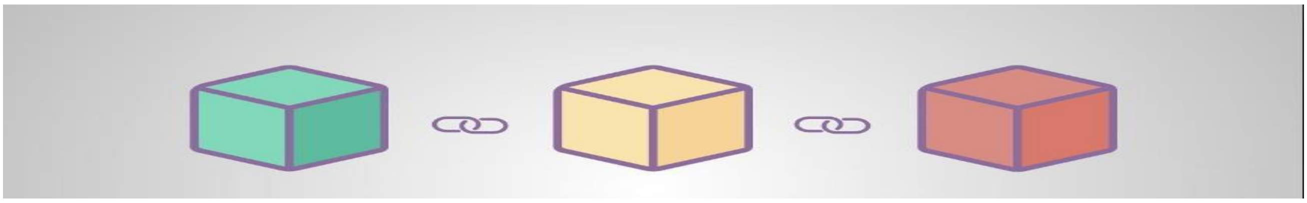


Fig: Blockchain

By grouping all the transactions details at prehash code for this and then store it in a block. Once the transaction is verified, then the block becomes permanent part of the blockchain, and chain keeps growing. So, it is believed that for every 10 minutes a new block is created and blockchain keeps growing accordingly. So, how many transactions happened to that all can be grouped as part of the block and then stored in to the blockchain block. Blockchain networks can be categorized based on their permission model, which determines who can maintain them (e.g., publish blocks). If anyone can publish a new block, it is permissionless. If only particular users can publish blocks, it is permissioned. In simple terms, a permissioned blockchain network is like a corporate intranet that is controlled, while a permission less blockchain network is like the public internet, where anyone can participate. Permissioned blockchain networks are often deployed for a group of organizations and individuals, typically referred to as a consortium.

PUBLIC LEDGERS:

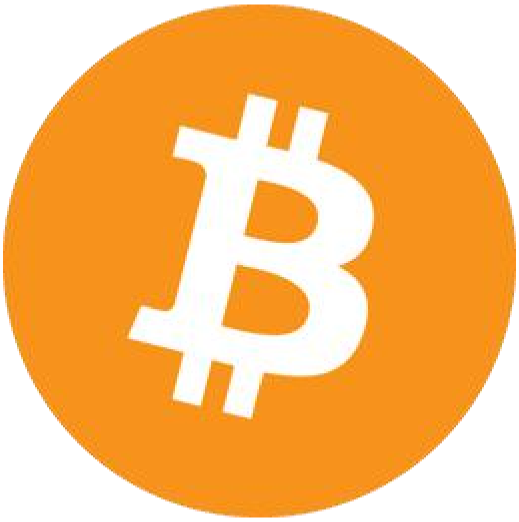
Public blockchain networks are decentralized ledger platforms open to anyone publishing blocks, without needing permission from any authority. Public blockchain platforms are often open source software, freely available to anyone who wishes to download them. Since anyone has the right to publish blocks, this results in the property that anyone can read the blockchain as well as issue transactions on the blockchain. Any blockchain network user within a public blockchain network can read and write to the ledger. Since public blockchain networks are open to all to participate, malicious users may attempt to publish blocks in a way that subverts the system.

PRIVATE LEDGERS:

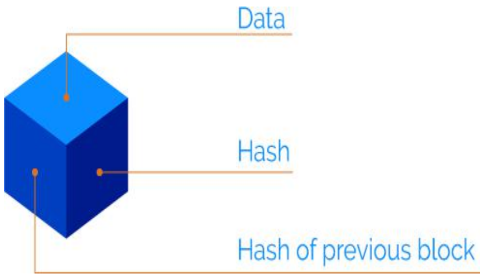
Private blockchain networks are ones where users publishing blocks must be authorized by some authority. Since only authorized users are maintaining the blockchain, it is possible to restrict read access and to restrict who can issue transactions.Private blockchain networks may thus allow anyone to read the blockchain or they may restrict read access to authorized individuals. They also may allow anyone to submit transactions to be included in the blockchain or, again, they may restrict this access only to authorized individuals. private blockchain networks may be instantiated and maintained using open source or closed source software.

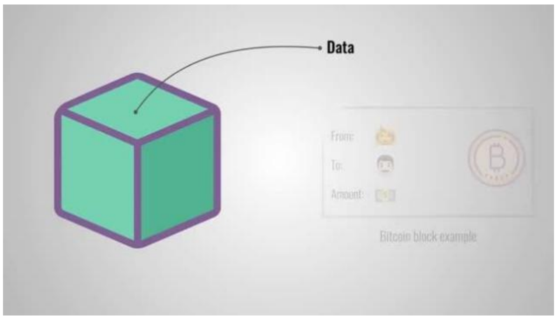
2.4 BITCOIN:

Bitcoin is the first decentralized digital currency that came into the market and was introduced in 2009 by — Satoshi Nakomoto. Bitcoins use various cryptographic and mathematical problems that ensure that the creation and management of bitcoins is restricted. Now the blockchain is a distributed ledger that is completely open to anyone , they have an interesting property, once in there is coded inside the blockchain it becomes very difficult to change it.

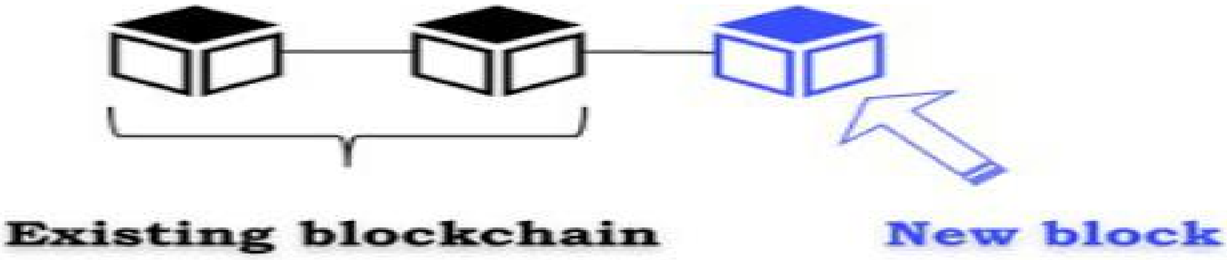


The bitcoin block example consists of three elements: One is the data which stores the data inside the block in the present type of blockchain. For example , the bitcoin blockchain stores the details about transactions, such as sender and receiver and the number of points.

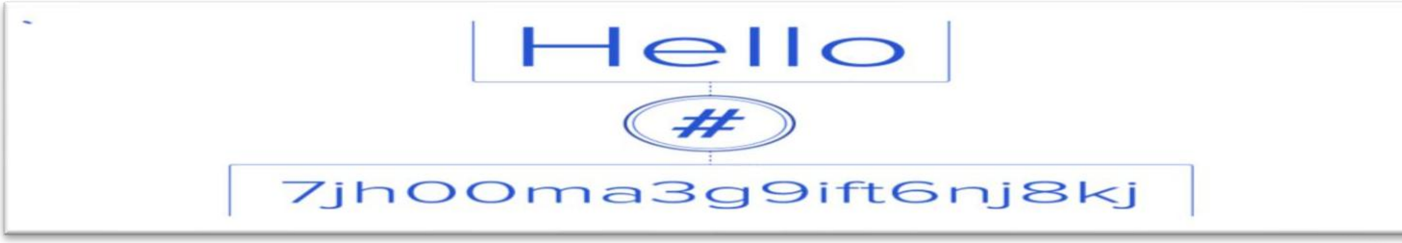




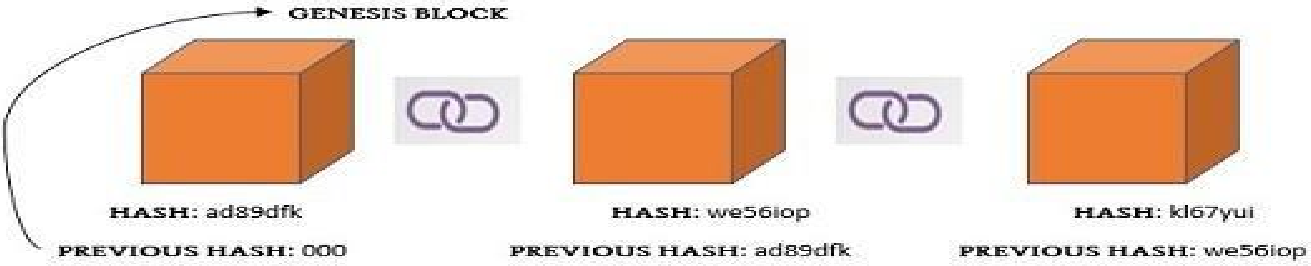
The Second is Hash, where the hash can be compared with a Fingerprint. It identifies a block and all of its contents and it is always unique just as a fingerprint.



Once a block is created, its hash is been calculated, changing something inside the block will cause hash to change. So, another words Hash is a failure one, when you wants to check the changes of the block. If the figure print of the block changes it no longer is the same block.



The third element inside of each block is the Hash of the previous block. This effectively creates a chain of blocks and this technique is used to keep this blockchain so secure.



`2.5 Cryptographic Hash Functions:

An important component of blockchain technology is the use of cryptographic hash functions for many operations. Hashing is a method of applying a cryptographic hash function to data, which calculates a relatively unique output (called a message digest, or just digest) for an input of nearly any size (e.g., a file, text, or image). It allows individuals to independently take input data, hash that data, and derive the same result – proving that there was no change in the data. Even the smallest change to the input (e.g., changing a single bit) will result in a completely different output digest. Table 1 shows simple examples of this.

Cryptographic hash functions have these important security properties:

1. They are preimage resistant. This means that they are one-way; it is computationally infeasible to compute the correct input value given some output value (e.g., given a digest, find x such that hash(x) = digest).

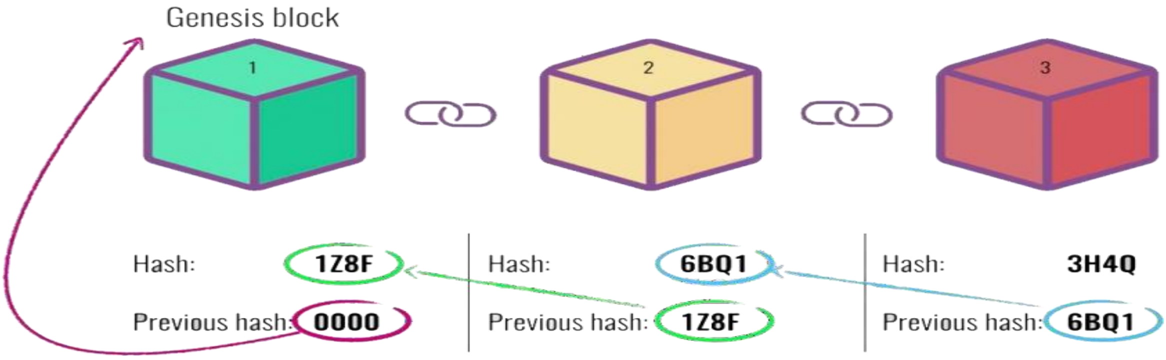
2. They are second preimage resistant. This means one cannot find an input that hashes to a specific output. More specifically, cryptographic hash functions are designed so that given a specific input, it is computationally infeasible to find a second input which produces the same output (e.g., given x, find y such that hash(x) = hash(y)). The only approach available is to exhaustively search the input space, but this is computationally infeasible to do with any chance of success.

3. They are collision resistant. This means that one cannot find two inputs that hash to the same output. More specifically, it is computationally infeasible to find any two inputs that produce the same digest (e.g., find an x and y which hash(x) = hash(y)). A specific cryptographic hash function used in many blockchain implementations is the Secure Hash Algorithm (SHA) with an output size of 256 bits (SHA-256). Many computers support this algorithm in hardware, making it fast to compute. SHA-256 has an output of 32 bytes (1 byte = 8 bits, 32 bytes = 256 bits), generally displayed as a 64-character hexadecimal string .

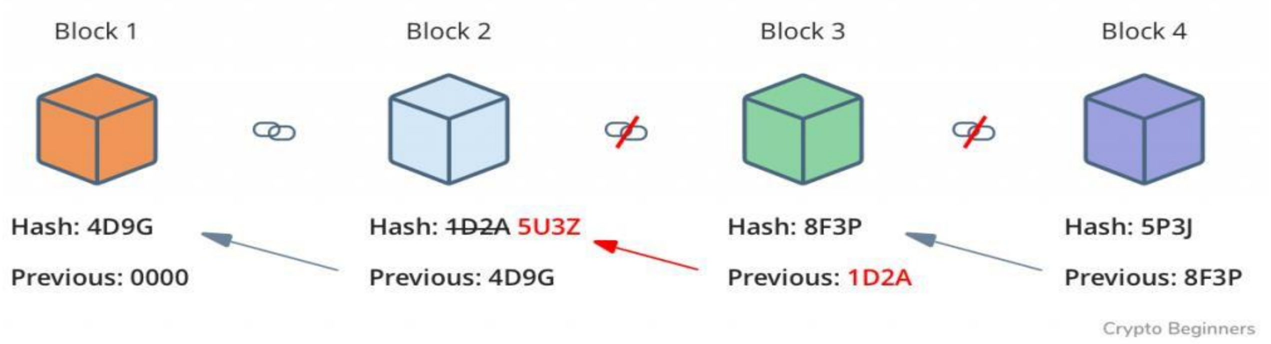
This means that there are 2^{256}, 10^{77}, or

115,792,089,237,316,195,423,570,985,008,687,907,853,269,984,665,640,564,039,457,584,00
7,913,129,639,936 possible digest values. The algorithm for SHA-256, as well as others, is specified in Federal Information Processing Standard (FIPS) 180-4 [5]. The NIST Secure Hashing website contains FIPS specifications for all NIST-approved hashing algorithms.

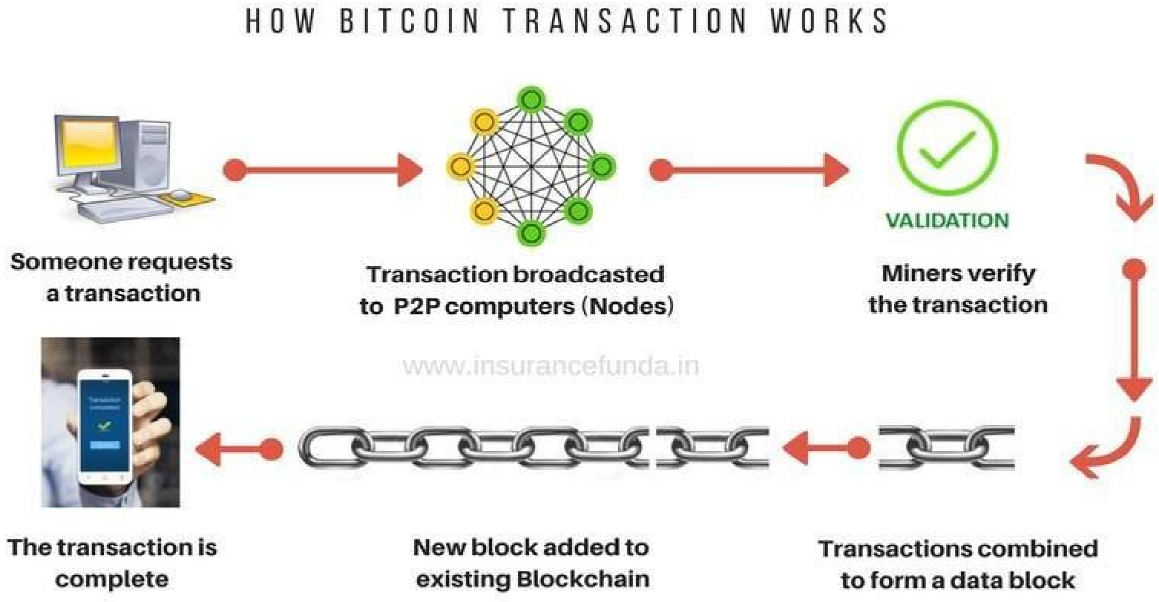
Let us take an example, here we have a chain of three blocks, as we can see each block has Hash and Previous hash,



Now the block No.3 points the block No.2 and bock No.2 points to No.1. The first block is a bit special, it can point to previous blocks, because well it's the first one, we call this block the—Genesis block. Now coming to the second block , it causes the hash of the block to changes well in turn the block 3 and all the following blocks invalid, because they no longer store a valid hash of the previous block. So, change in the single block will make all following blocks invalid. But using hash is none enough to prevent tempering.



Computing these days are very fast and can calculate 100's of, 1000's of hashes per second , we could effectively tamper with the block and we calculate all the hashes of the other blocks to make the blockchain family again. So, to mitigate this blockchain are something that are called Proof-of-Work. It is a mechanism that slows down the creations of new blocks. In Bitcoins case it takes about 10 minutes to calculate the coin Proof – of – Work and add a new block to the chain. This mechanism makes a very hard to tamper with the blocks , because if we tamper with one block, we need to calculate the proof –of-work for all the following blocks. So, the security of a blockchain comes from the creatives of the hashing and the proof-of-work mechanism. There is one more way, Blockchains secured themselves, that is being distributed.


HOW BITCOIN TRANSACTION WORKS
Someone requests a transaction
Transaction broadcasted to P2P computers (Nodes)
VALIDATION
Miners verify the transaction
www.insurancefunda.in
The transaction is complete
New block added to existing Blockchain
Transactions combined to form a data block

Bitcoin Transaction Management:

Now Blockchain and Bitcoin are some most of trendy keywords as part of the today’s technology and even those who are not familiar with crypto currency are quite impressed in the same. Blockchain is been used highly for transaction management and it is replacing the current existing transaction management system. If a technology is replacing the existing system, there must be a certain problem.

Issues with Current Banking Systems :

For example, When Host A wants to send $100 to Host B, due to transaction fee $2, Host B is getting only $98, now it may not seem a huge amount but lets assume that there are every day 10 thousand transactions are happen, and in that 10 thousand transactions and if 2% commission and it’s a huge amount. Some of the issues like, Net Banking Frauds, Transactional Charge with everything and Financial crises etc.,

Smart contracts:

The term smart contract dates to 1994, defined by Nick Szabo as “a computerized transaction protocol that executes the terms of a contract. The general objectives of smart contract design are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries.” A smart contract is a collection of code and data (sometimes referred to as functions and state) that is deployed using cryptographically signed transactions on the blockchain network (e.g., Ethereum’s smart contracts, Hyperledger Fabric’s chaincode). The smart contract is executed by nodes within the blockchain network; all nodes that execute the smart contract must derive the same results from the execution, and the results of execution are recorded on the blockchain.

3.CONCLUSION AND FUTURE SCOPE

Blockchain technology is a new tool with potential applications for organizations, enabling secure transactions without the need for a central authority. Starting in 200913, with Bitcoin leveraging blockchain technology, there has been an increasing number of blockchain technology-based solutions. The first applications were electronic cash systems with the distribution of a global ledger containing all transactions. These transactions are secured with cryptographic hashes, and transactions are signed and verified using asymmetric-key pairs. The transaction history efficiently and securely records a chain of events in a way that any attempt to edit or change a past transaction will also require a recalculation of all subsequent blocks of transactions. The use of blockchain technology is still in its early stages, but it is built on widely understood and sound cryptographic principles.

Currently, there is a lot of hype around the technology, and many proposed uses for it. Moving forward, it is likely that the hype will die down, and blockchain technology will become just another tool that can be used. As detailed throughout this publication, a blockchain relies on existing network, cryptographic, and recordkeeping technologies but uses them in a new manner. It will be important that organizations are able to look at the technologies and both the advantages and disadvantages of using them. Once a blockchain is implemented and widely adopted, it may become difficult to change it. Once data is recorded in a blockchain, that data is usually there forever, even when there is a mistake. Applications that utilize the blockchain as a data layer work around the fact that the actual blockchain data cannot be altered by making later blocks and transactions act as updates or modifications to earlier blocks and transactions.

This software abstraction allows for modifications to working data, while providing a full history of changes. For some organizations these are desirable features. For others, these may be deal breakers preventing the adoption of blockchain technology. Blockchain technology is still new and organizations should treat blockchain technology like they would any other technological solution at their disposal--use it only in appropriate situations.

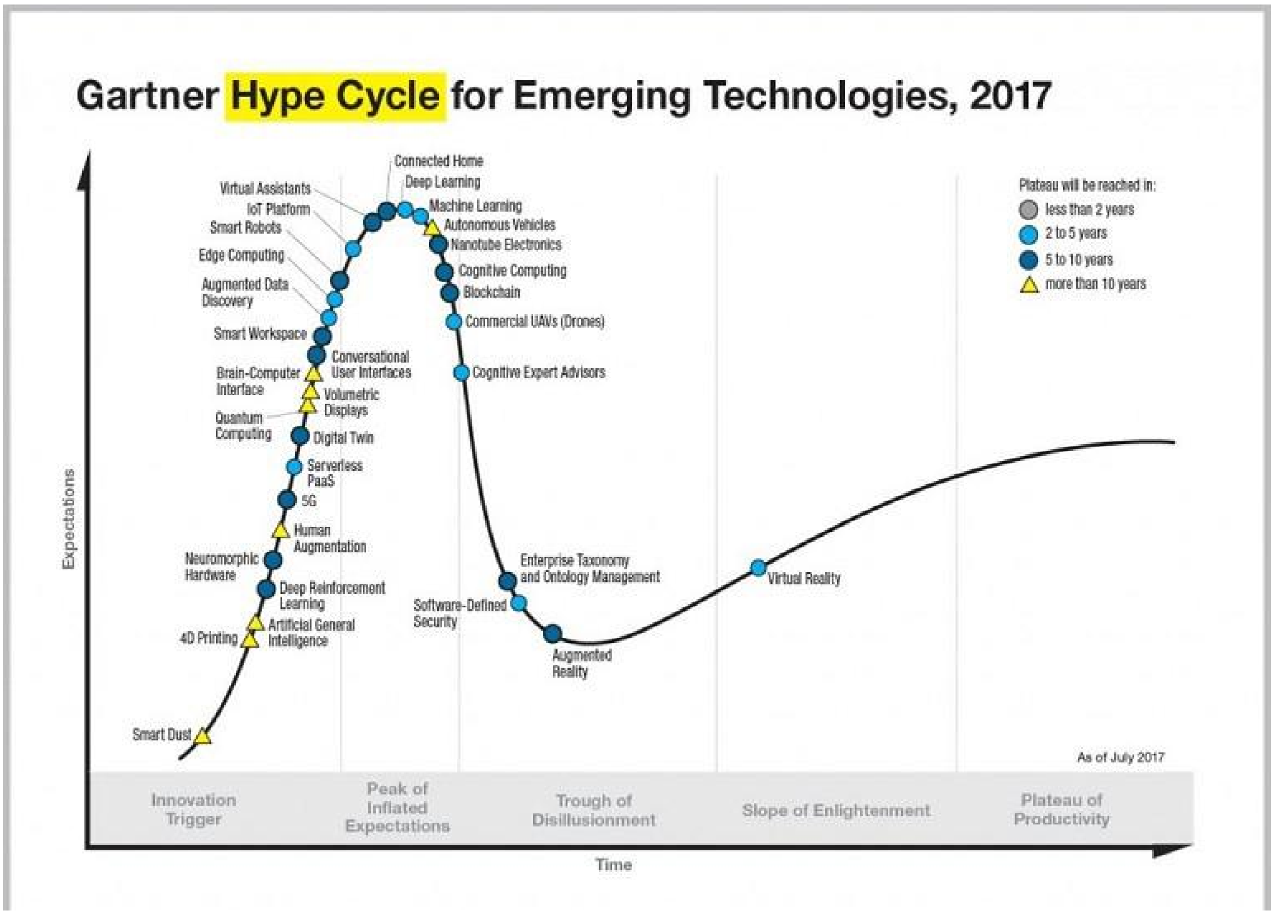


Fig : Future scope of block chain

According to the Gartner Hype Cycle for Emerging Technologies 2017, shown in Figure above, Blockchain still remains in the region of “Peak of Inflated Expectation” with forecast to reach plateau in “five to ten years”. However, this technology is shown going downhill into the region of the “Trough of Disillusionment”. Because of the wide adoption of the Blockchain in a wide range of applications beyond cryptocurrency, the authors of this paper are forecasting a shift in classification from “five to ten years” to “two to five years” to reach maturation. Blockchain possesses a great potential in empowering the citizens of the developing countries if widely adopted by e-governance applications for identity management, asset ownership transfer of precious commodities such as gold, silver and diamond, healthcare and other commercial uses as well as in financial inclusion. However, this will strongly depend on national political decisions.

REFERENCES

1. Attiya, H. and Welch, J. Distributed Computing:Fundamentals, Simulations and Advanced Topics.John Wiley & Sons, 2004.

2.Buterin, V. and Griffith, V. Casper the Friendly FinalityGadget, (2017);https://github.com/ethereum/research/commits/master/papers/casper-basics/ casper_basics.pdf.

3. Cachinm, C. and Vukolic, M. Blockchain consensus protocols in the wild (Keynote Talk). In Proceedings of the 31st International Symposium on Distributed Computing. Andréa W. Richa, ed. (2017), 1:1–1:16.