



"A Survey: Blockchain"

Vaibhavi Shukla¹

Computer Engineering Department, Shgec, Amreli, India¹

Abstract: Blockchain- The Blockchain is alleged to be the technology of future. Despite the inherent 'Block' in it, the name has traversed additional miles than the other technical term within the recent past. it's reverberant in nearly all existing IT infrastructures; move a possible threat to the very existence of the present institutions.

Keywords: Blockchain, Applications, Ledger, Bitcoin

I. INTRODUCTION

With the invention of Bitcoin in 2008, the globe was introduced to a brand new idea, that is currently probably to revolutionize the entire of society. it's one thing that guarantees to own an effect on each business, including but not restricted to the money sector, government, media, law, and arts. A Blockchain is a digital ledger of transactions that's duplicated and distributed across the complete network of pc systems on the Blockchain. each & every block within the chain contains variety of transactions, and each time a brand new dealing happens on the Blockchain, a record of that dealing is additional to each participant's ledger. The localized information managed by multiple participants is understood as Distributed Ledger Technology (DLT).Blockchain is a type of DLT i.e. Distributed Ledger Technology in which transactions are recorded with an immutable cryptographic signature called a hash.

Bitcoin has many blessings over alternative current transaction systems, together with the following:

TABLE I Advantages over current transaction systems

Sr No	Advantages over current transaction systems
1. Cost-effective:	Bitcoin eliminates the necessity for intermediaries.
2. Efficient:	dealing info is recorded once and is available to all or any parties through the distributed network.
3. Safe and secure:	The underlying ledger is tamper-evident. A dealing cannot be changed; it can solely be reversed with another dealing, within which case each transactions are visible.

Bitcoin and Blockchain are not same. Bitcoin and Blockchain are usually used interchangeably, however they're not a similar thing. Bitcoin is, rather, an application of Blockchain technology. Think of it like Google and also the web. Google runs on the web and would not exist without it, however the web still exists without Google. Likewise, Bitcoin would not exist without Blockchain, however they don't seem to be synonymous .

TABLE III Difference between Bitcoin and Blockchain

Key points	Bitcoin	Blockchain
1. What is it?	A crypto-currency	A ledger
2. Main Aim	To simplify & increase the speed of transactions without much of government restrictions.	To provide low cost, safe, secure environment for peer to peer transactions.
3. Strategy	Bitcoin focuses on lowering the cost of influencers & reduces the time of transactions but is less flexible	Blockchain can be adapted to any change & hence it can use in different industries
4. central - distributed	There is no central bank or single administrator for Bitcoins, as a result, they can be sent from user to user on the peer-to-peer Bitcoin network without the need for intermediaries.	It allows to record transactions between two parties efficiently and in a verifiable and permanent way.

5.	Real world use	Is limited to trading as a currency.	It Can be used to transfer anything of value, from currencies to property titles or stocks among others. Blockchain technologies have countless uses in both private and public sector
6.	Scope	Has a more limited scope	More and more governments are launching Blockchain initiatives and opting for this technology to guarantee the trust, transparency and security of their systems.
7.		Bitcoin is a crypto currency	Blockchain is a distributed database
8.		Bitcoin promotes anonymity	Blockchain is about transparency

II. LITERATURE SURVEY

History of Blockchain:

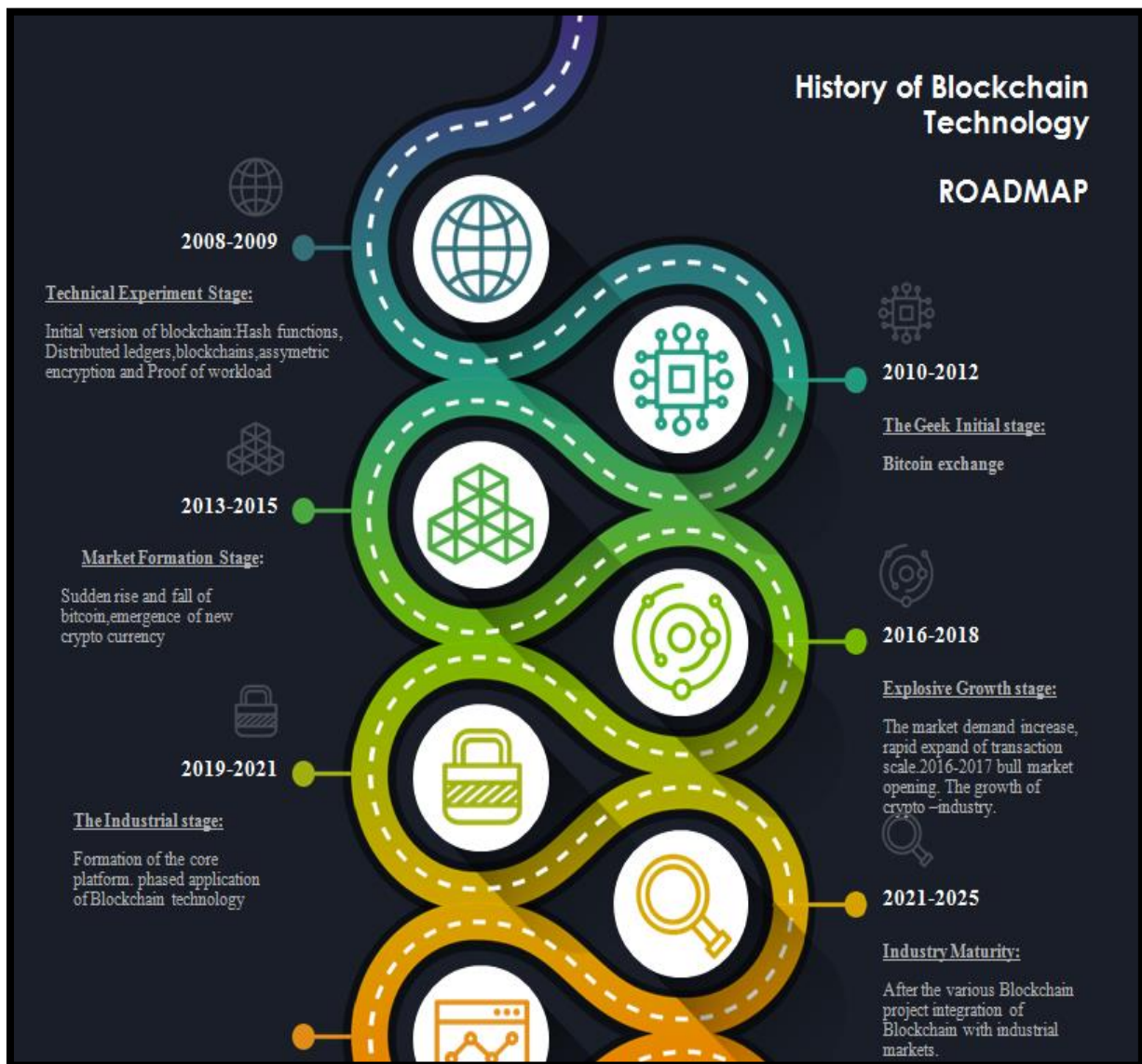
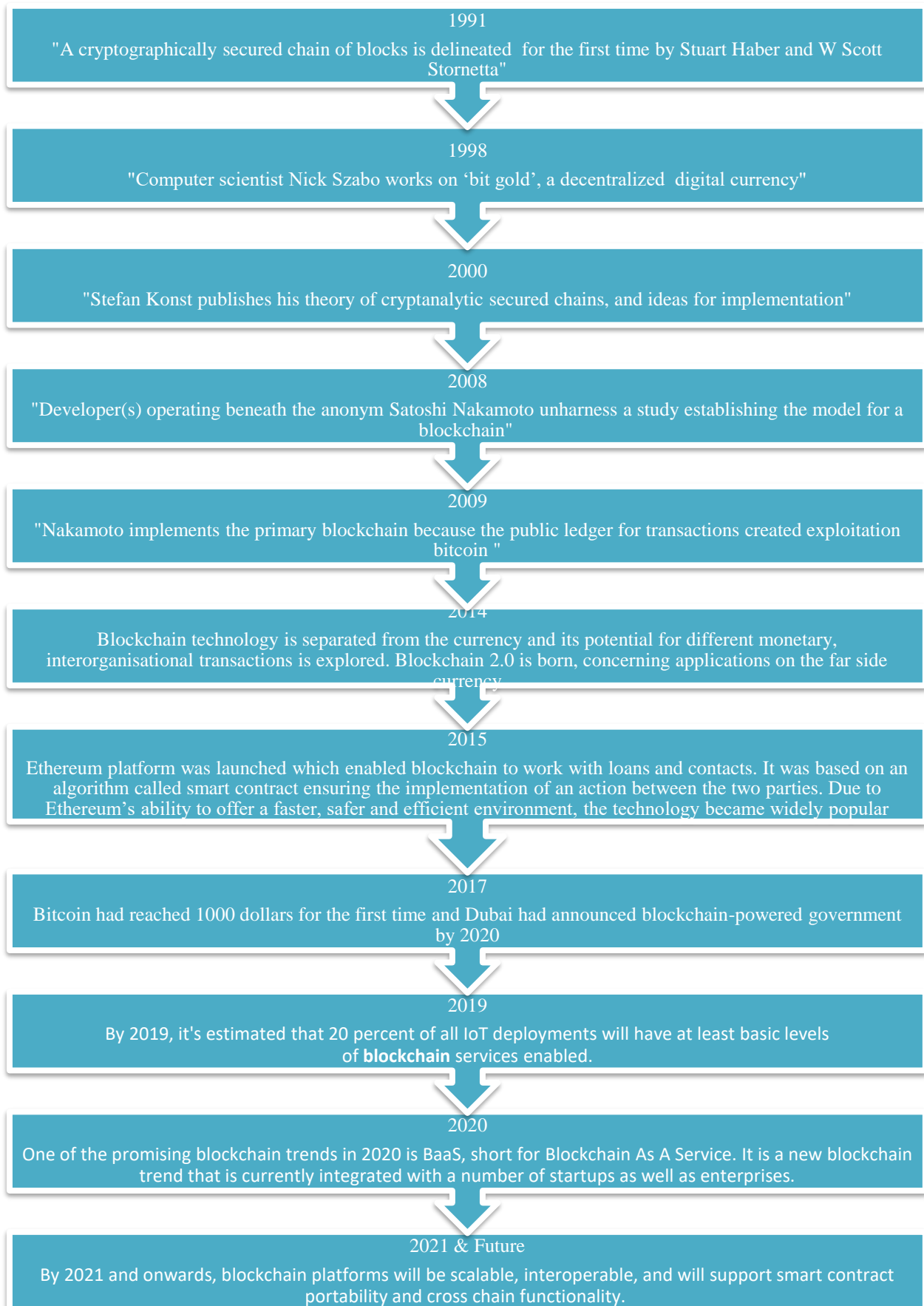


Fig. 1 History of Blockchain



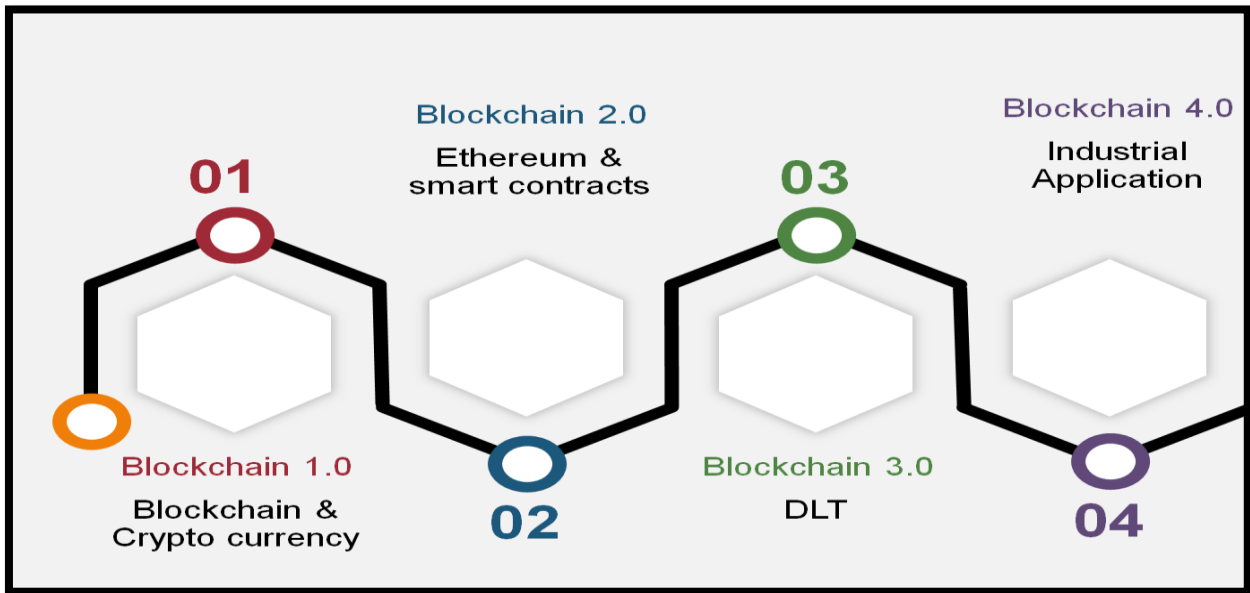


Fig. 2 - Revolution of Blockchain

Blockchain 1.0 - Blockchain & crypto currency:

A crypto currency is a form of digital asset based on a network that is distributed across a large number of computers. This decentralized structure allows them to exist outside the control of governments and central authorities. The word “crypto currency” is derived from the encryption techniques which are used to secure the network. Basically, a digital asset, Blockchain crypto currency is designed to work as a medium of exchange. Unlike physical currencies, Blockchain crypto currency works on digital channels and are often adhered to strong cryptography to secure financial transactions that happen online. These cryptographs or encryption layers may also be used to control the creation of additional units and verify the transfer of assets. Blockchain crypto currency can have several types. They are Bitcoin, Lit coin, Ripple, Ether, etc.

TABLE III Blockchain & crypto currency

Basis of Comparison	Blockchain	Cryptocurrency
Nature	A technology that records transactions	Tools used in virtual exchanges
Use	Record transactions	Make payments, investments, and storage of wealth
Value	Have monetary value	Have no monetary value
Mobility	Can be transferred	Can't be transferred

Blockchain 2.0 - Ethereum & smart contracts: Ethereum is an open source Blockchain that was officially launched in 2015. A smart contract is executable code that runs on top of the Blockchain to facilitate, execute and enforce an agreement between untrusted parties while not the involvement of a trusty third party. Ethereum could be a decentralised, open supply, and distributed computing platform that allows the creation of sensible contracts and decentralised applications. Smart contracts are laptop protocols that facilitate, verify, or enforce the negotiation and performance of some type of agreement. a wise contract is just about precisely what you're thinking that it'd be: it's associate auto-executing, programmed agreement that's recorded on the Ethereum Blockchain. It operates primarily based upon associate if, then logic, in order that if x action happens, then y action happens. "Smart contracts are applications that run precisely as programmed with none risk of period, censorship, fraud or third-party interference." Let's break down what all that means:

- Downtime: the applications ne'er close up unexpectedly and may ne'er be transitioned.
- Censorship: Ethereum nodes (computers running the protocol) are distributed round the world eliminating censorship from a central authority.
- Fraud: the contract can't be modified, hacked, or manipulated.
- Third parties: the contract self-executes and thus doesn't need associate negotiated.

Blockchain 3.0 - DLT : Distributed Ledger Technology (DLT) refers to the technological infrastructure and protocols that permits co-occurring access, validation, and record change in an changeless manner across a network that is spread across multiple entities or locations. In easy words, the DLT is all regarding the concept of a "decentralized" network against the standard "centralized" mechanism, and it's deemed to possess comprehensive implications on sectors and entities that have long relied upon a sure third-party. DLT permits for storage of all info in a very secure and correct manner exploitation cryptography. an equivalent are often accessed exploitation "keys" and science signatures. Once the knowledge is hold on, it becomes an changeless information and is ruled by the principles of the network.

Advantages of DLT:-

- In DLT, information is 100% tamper proof until the information ledger is distributed.
- It offers extremely secure and trustworthy expertise.
- A decentralised non-public distributed network enhances the strength of the system and assures continuous operation with none interruption. Every Blockchain may be a distributed ledger, however not each distributed ledger may be a Blockchain.

Blockchain 4.0 - Industrial Application : By adopting the vision of industry 4.0, several industrial sectors are eyeing the potential for advancing their systems to attain higher productivity, cost-effectiveness, reliableness, quality, and adaptability.

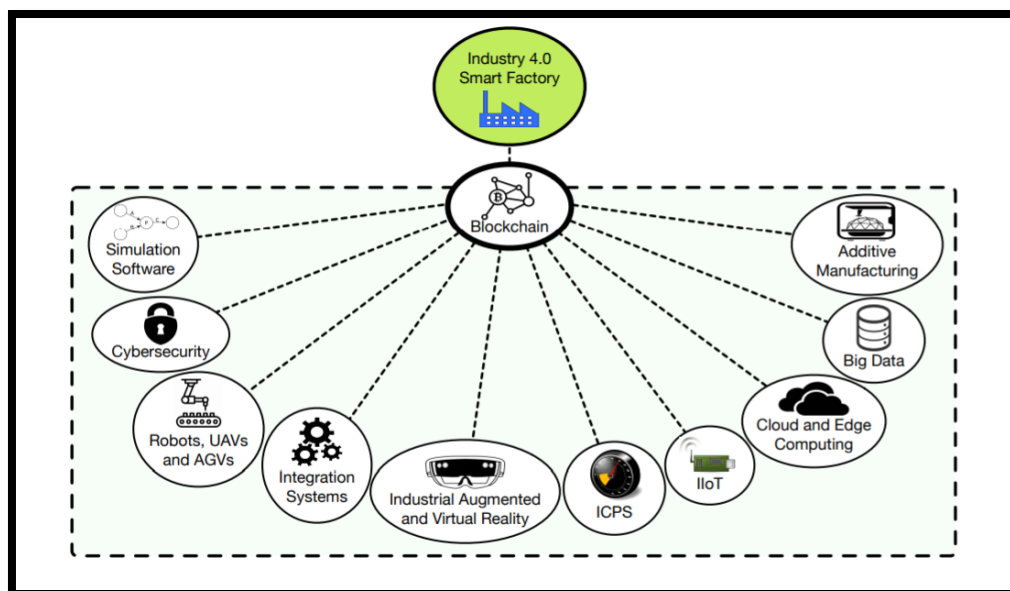


Fig. 3 - Industrial Applications of Blockchain

Blockchain is a combination of three leading technologies:

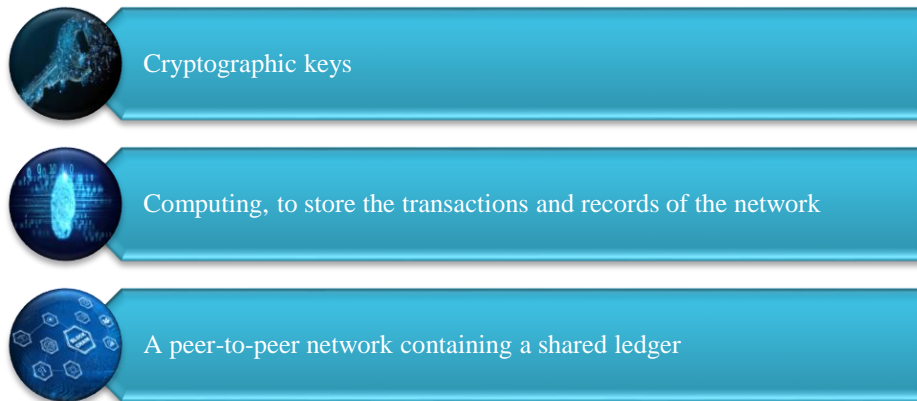


Fig. 4 - Leading technologies of Blockchain

These are the core Blockchain architecture components:

- **Node** — user or computer within the Blockchain
- **Transaction** — smallest building block of a Blockchain system
- **Block** — a data structure used for keeping a set of transactions which is distributed to all nodes in the network
- **Chain** — a sequence of blocks in a specific order
- **Miners** — specific nodes which perform the block verification process
- **Consensus** — a set of rules and arrangements to carry out Blockchain operations

There are 3 important concepts in Blockchain:

❖ **Blocks:** Data is kept digitally in a record referred to as a 'block'. This block contains:

- **Block header:** info concerning the block, like a singular block reference variety – the hash. The header conjointly includes, the hash of the previous block and also the time the block was created.
- **Block content:** the record itself, for instance, info a few dealings. The block acts sort of a ledger entry for this transaction.

A block represents the 'present' and contains data regarding its past and future. on every occasion a block is completed it becomes a part of the past and provides way to a new block within the Blockchain. the completed block may be a permanent record of transactions within the past and also the new transactions square measure recorded within the current one. This way, the full system works in a very cycle and knowledge gets for good keep. every block includes records of some or all recent transactions, and a regard to the block that preceded it that, beside Bitcoins peer-to-peer verification system, makes it nearly not possible for a user to tamper with previously recorded transaction information.

❖ **Nodes:** In general, each participant during a coin's network could be a node. you've got 2 kinds of nodes. Full nodes that store a duplicate Blockchain and so guarantee the protection and correctness of knowledge the info the information} on the Blockchain by validating data. The second sort could be a light-weight node – every user collaborating, who must connect with a full node so as to synchronize to this state of the network and be able to participate.

Node has two more jobs:

- Sharing information.
- Keeping a copy of confirmed transactions.

When a miner makes an attempt to add a new block of transactions to the Blockchain, it broadcasts the block to all or any the nodes on the network. based on the block's legitimacy (validity of signature and transactions), nodes will

accept or reject the block. once a node accepts a new block of transactions, it saves and stores it on top of the rest of the blocks it already has stored. In short, here is what nodes do: Nodes check if a block of transactions is valid and accept or reject it. Nodes save and store blocks of transactions (storing Blockchain transaction history). Nodes broadcast and spread this dealing history to different nodes that will got to synchronize with the Blockchain (need to be updated on transaction history).

❖ **Miners:** Miners may be outlined as accountants who records each transactions to the Blockchain. The idea is easy, a proof of payment is very important if you would like your payment to be valid. The miners are those who keep the record of your payment. thus they're record keepers who keep the system updated of recent payments and existing ones. When you issue a payment to somebody in Bitcoin, you're really announcing that you just wish this several Bitcoins transferred to a different account. Then announcement is created by receiver to the Blockchain network. The nodes within the network makes note of this announcement and cross checks the payment with each transactional knowledge on the network. this is often done by checking if the user has used a similar coin in alternative transactions at a similar time. thus this method with success eliminates double outlay. If there are not any matches, then the nodes can announce this transfer to the miner network. Now the miner's task is to feature the dealings to the Blockchain. however if all the mineworker add the dealings to the Blockchain at a similar time, there'll be, multiple records of a similar dealings. So what miners do is race one another to verify a block. Before they'll enter a block, they should solve it. The blocks are encrypted with an cryptography code that works on SHA-256 rule. This cryptography is termed a hash. thus if you would like to resolve and add a block you wish to resolve the cryptography by coming into the right key. The miners really work out this key with pure guess. however they don't have to do it themselves! The computers process power is employed to come back up with the solution for the coding. therefore the computers return up with a series of various combination to suit the cryptography. The first miner to resolve the hash or the coding decision add the block to the present Blockchain. Once the nodes on the network settle for the new block, the payment gets confirmed. Once a block is added to the network, the miner receives many Bitcoins and a small add as reward for the time and resources he or she had unconditional into the mining method.

Some key points of Blockchain:

- ❖ Blockchain may be a specific variety of db.
- ❖ It differs from a typical info within the method it stores information; Blockchain store information in blocks that area unit then bound along.
- ❖ As new information comes in its entered into a recent block. Once the block is crammed with information it's bound onto the previous block, that makes the information bound along in written record order.
- ❖ Different types of knowledge will be hold on on a Blockchain however the foremost common use up to now has been as a ledger for transactions.
- ❖ In Bit coin's case, Blockchain is employed in a very localized method so no single person or cluster has control—rather, all users together retain management.
- ❖ Decentralized Blockchain are immutable , which implies that the information entered is irreversible. For Bitcoin, this suggests that transactions area unit for good recorded and visible to anyone.

Basic features of Blockchain Technology:

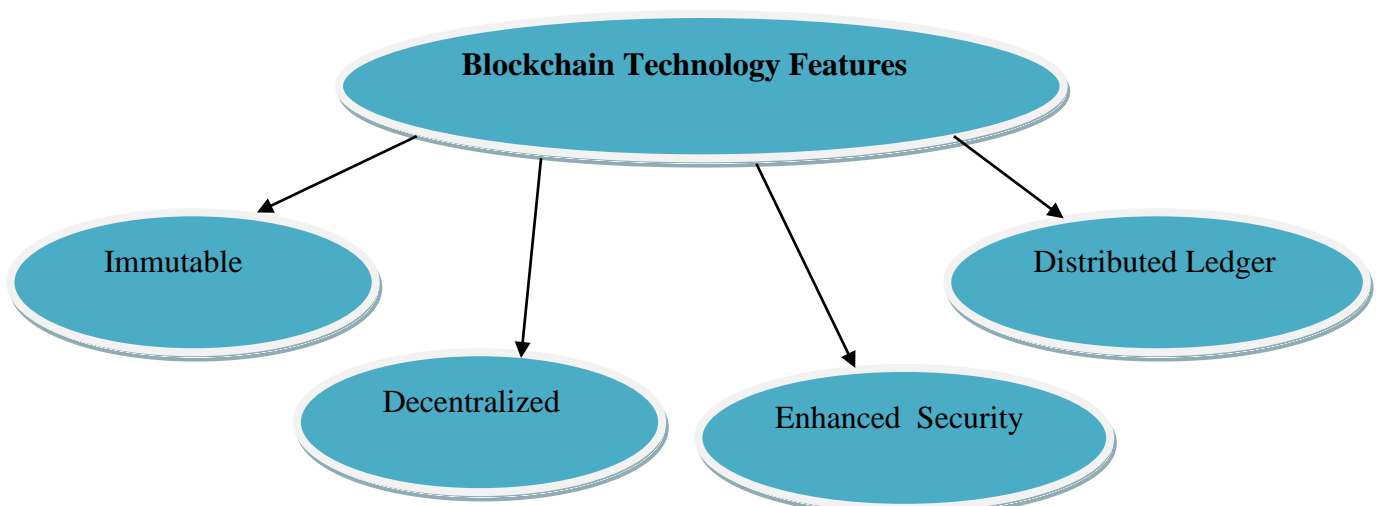


Fig. 5 Features of Blockchain Technology



1. Immutable

It implies that no Blockchain developer or user will alter/delete the info within the ledger or add new content with none validation. This feature ensures unchangeability. In reality, the Blockchain group action works slightly otherwise than the other monetary company. because it doesn't have any centralized authority, it depends on the node inside the network. When a Blockchain group action happens, all the nodes within the network can need to say it's valid or won't get additional to the ledger. Moreover, once a block is additional, it's permanent. Thus, there's no method of adjusting it or fixing it.

2. Decentralized

Gets eliminate human-made errors, thus it's a lot of fault-tolerant. More management for users over their properties. Highly secure as a result of its costlier, a lot of hackers to stack the system. Gets eliminate all third-party integrations. No probability of being scammed because the system runs entirely on algorithms. Every modification is reviewed by the nodes, that promotes transparency.

3. Enhanced Security

There's no way to crack the code. what is more, if anyone desires to vary any value within the block, it'll generate a totally different outcome that won't be coupled to the first modification. in addition, each block comes with a singular hash ID. However, dynamical the hash ID is not possible.

4. Distributed Ledger

High response time for any malicious activity because any change in the ledger is detectable relatively faster. So, it's easy to track what's the issue. The nodes act as the verifiers, and so it offers them a role of participation. It gets rid of any favours in the network. And so, everyone will get an equal amount of privileges in the system.

Application of Blockchain:

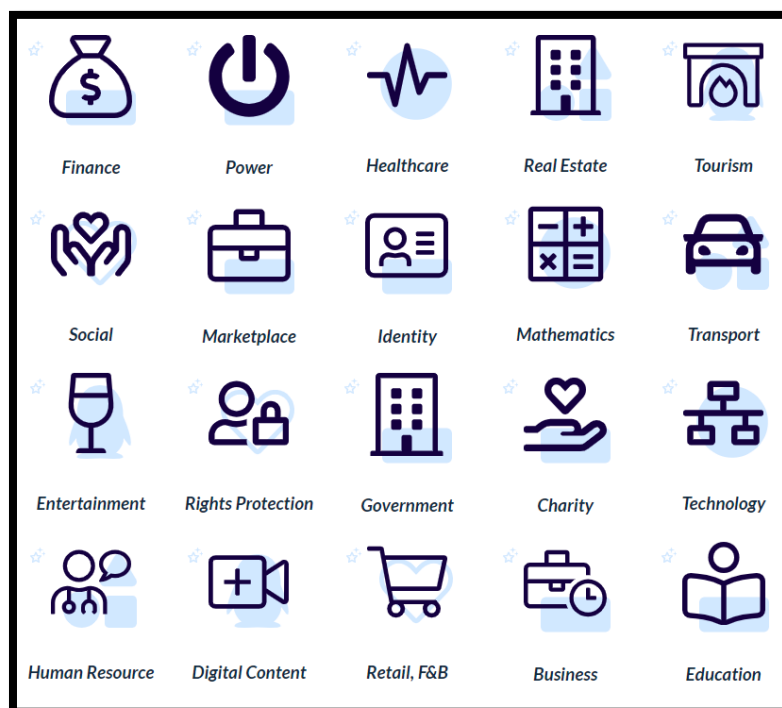

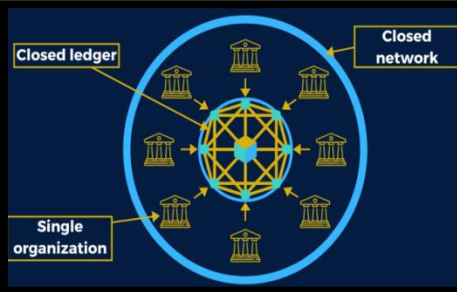


Fig. 6 Features of Blockchain Technology

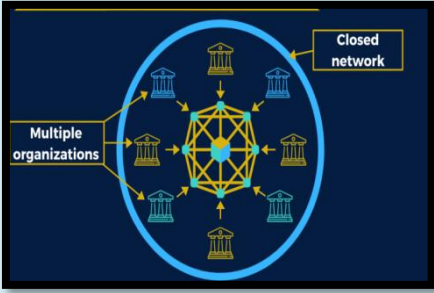


Types of Blockchain

TABLE IV Different types of Blockchain

Sr No.	Advantages	Disadvantages
<p>1. Public Blockchain</p> <ul style="list-style-type: none"> Anyone is allowed to join and participate in the consensus Fully decentralized secure and immutable Ledge system Transaction are anonymous but transparent to everyone  <p>Fig: Public Blockchain</p> <p>USE CASES:</p> <p>Voting: Governments can do voting through public Blockchain employing transparency and trust.</p> <p>Fundraising: Companies or initiatives can make use of the public Blockchain for improving transparency and trust.</p>	<p>Anyone will be a part of the public Blockchain.</p> <p>It brings trust among the complete community of users</p> <p>Everyone feels incentivized to figure towards the betterment of the public network</p> <p>Public Blockchain needs no intermediaries to figure.</p> <p>Public Blockchain also are secure looking on the quantity of collaborating nodes</p> <p>It brings transparency to the complete network because the offered information is out there for verification purposes.</p>	<p>They suffer from a lack of transaction speed.</p> <p>Scalability</p>
<p>2. Private Blockchain</p> <ul style="list-style-type: none"> A single organisation will have authority over the network Faster output, power efficient and offers privacy Simplified data handling process not open to everyone  <p>Fig: Private Blockchain</p>	<p>Private Blockchain are quick. this is often as a result of there are few participants compared to the general public Blockchain. In short, it takes less time for the network to succeed in accord leading to quicker transactions.</p> <p>Private Blockchain are more scalable as compared to public. The scalability is possible because, in a private Blockchain, only a few nodes are authorized to validate transactions.</p>	<p>Private Blockchain are not truly decentralized.</p> <p>As there are only a few nodes here, the security isn't all that good.</p>



<p>USE CASES:</p> <p>Supply chain management: Organizations can deploy a private Blockchain to manage their supply chain. Asset ownership: Assets can be tracked and verified using a private Blockchain.</p> <p>Internal Voting: Private Blockchain is also effective at internal voting.</p>		
<p>Federated Blockchain</p> <ul style="list-style-type: none"> Multiple organisations influences the Blockchain network Decentralized, extremely fast and scalable system Network regulations preserves security and privacy  <p>Fig: Federated Blockchain</p> <p>USE CASES:</p> <p>Banking and payments: A group of banks can work together and create a consortium. They can decide the nodes that will validate transactions.</p> <p>Research: A consortium Blockchain can be used to share research data and results. Food tracking: It is also great for food tracking.</p>	<p>It offers higher customizability and management over resources.</p> <p>Safer and have higher quantifiability.</p> <p>It is additionally additional economical compared to public Blockchain networks.</p> <p>Works with well-defined governance structures. It offers access controls.</p>	<p>Even though it's secure, the total network will be compromised thanks to the member's integrity.</p> <p>It is less clear.</p> <p>Regulations and censorship will have a large impact on network practicality.</p> <p>It is conjointly less anonymous compared to alternative forms of Blockchain.</p>
<p>Hybrid Blockchain</p> <ul style="list-style-type: none"> Authoritative access, only certain elements are private Flexible control over What data is kept public and private Decentralized, regulated and highly scalable system 	<p>Works in an exceedingly closed scheme while not the requirement to create everything public.</p> <p>Rules will be modified consistent with the wants.</p> <p>Hybrid networks also are proof against fifty one attacks.</p> <p>It offers privacy whereas still connected with a public network.</p> <p>It offers sensible measurability compared to the general public network.</p>	<p>Not fully transparent.</p> <p>Upgrading to the hybrid Blockchain are often a challenge.</p> <p>There is no incentive for taking part and contributively to the network.</p>

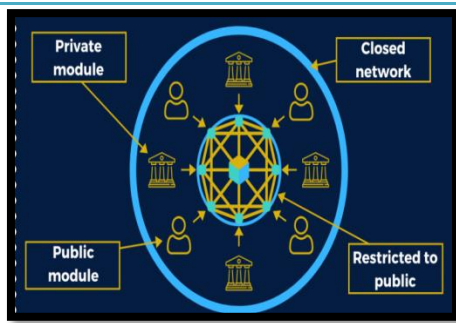


Fig: Hybrid Blockchain

USE CASES:

Real estate: you'll be able to use hybrid networks for real-estate functions wherever real-estate corporations can use it to run their systems and use the general public to point out info to the general public.

Retail: Retail may also use the hybrid network to contour their processes.

Highly regulated markets: Hybrid Blockchain also are ideal for extremely regulated markets like monetary markets.

Advantages of Blockchain

1. Security is taken into account one among the numerous benefits of this technology.
2. It's nearly not possible to corrupt a Blockchain as a result of the knowledge is shared and frequently reconciled by thousands, even millions, of computers, and Blockchain has no single purpose of failure.
3. Transactions area unit economical.
4. It's not a problem if one node goes down as a result of all the opposite nodes have a duplicate of the ledger. Confirmed blocks area unit terribly troublesome to reverse, which means registered knowledge is incredibly troublesome to get rid of or modification.
5. Costs ought to be reduced as a result of there's no want for reliance on third-party

Disadvantages of Blockchain

1. The main disadvantage of the Blockchain is the high energy consumption
2. The signature verification is the challenge of the Blockchain, because each transaction must be signed with cryptographic scheme, the big computing power is necessary for the calculation process to the sign. It is the one of the reasons to the high energy consumption
3. The high costs are a big disadvantage of the Blockchain

III.CONCLUSION

It is necessary to stay exploring the Blockchain development and application within the totally different areas for the nearest future, as a result of this new technology will facilitate to resolve many tough issues, that are troubling and preventing correctly systems work

**REFERENCES**

- [1]. Wubing Chen, Zhiying Xu, Yang Zhao and Jun Zhao "A Survey of Blockchain Applications in Different Domains" in research gate, International Conference 2018.
- [2]. Conoscenti, M., Vetro, A., and De Martin, J. C. Blockchain for the Internet of Things: A systematic literature review. In IEEE/ACS International Conference of Computer Systems and Applications (AICCSA) 2016.
- [3]. Jameela Al-Jaroodi, (Member, Ieee), And Nader Mohamed "Blockchain in Industries: Survey" in IEEE Volume 7, 2019.
- [4]. Tejasvi Alladi, Vinay Chamola, Reza M. Parizi, And Kim-Kwang Raymond Choo "Blockchain Applications for Industry 4.0 and Industrial IoT: A Review" in IEEE Volume 7, 2019
- [5]. Xiaoqi Li, Peng Jiang, Ting Chen, Xiapu Luo , Qiaoyan Wen "A survey on the security of Blockchain systems" Elsevier Future Generation Computer Systems,2020.
- [6]. Charles Shen And Feniosky Pena-Mora "Blockchain for cities_a systematic Literature review" in IEEE,November 12, 2018.
- [7]. Tiago m. Fernández-caramés and paula fraga-lamas,"A Review on the Use of Blockchain for the Internet of Things" in IEEE,May 31, 2018.
- [8]. Shailak Jani "The Emergence of Blockchain Technology & its Adoption in India",in Research gate,July 2019.
- [9]. Roberto Tonelli , Marco Ortu and Andrea Pinna Special Issue "Advances in Blockchain Technology and Applications 2020" in Research gate April 2020.
- [10]. Taghreed Justinia ,"Blockchain Technologies: Opportunities for Solving Real-World Problems in Healthcare and Biomedical Sciences" in review / acta inform med. 2019 dec 27.
- [11]. Zibin Zheng and Shaoan Xie, Hong-Ning Dai, Xiangping Chen and Huaimin Wang"Blockchain challenges and opportunities: a survey" in Int. J. Web and Grid Services, Vol. 14, No. 4, 2018.
- [12]. Ashish Sharma and Dinesh Bhuriya "Literature Review of Blockchain Technology" in IJRAR- International Journal of Research and Analytical Reviews, march 2019.
- [13]. Sana Sabah, Nada Mahdi and Israa Majeed " The road to the blockchain technology: Concept and types" in Research gate December 2019.
- [14]. Erik sakk and shuangbao " Integration of Blockchain Concepts into Computer Science Curriculum" in Journal of The Colloquium for Information Systems Security Education, Volume 8, No. 1, Fall 2020.