International Journal of Aquatic Science
ISSN: 2008-8019
Vol 12, Issue 01, 2021

Empirical View Of Financial Management Survey In Block Chain Technology Issues, Risk And Mitigation

Ashwini N[1], Sumangala Biradar[2], Kattupalli Sudhakar[3], Dr.B.Indira[4],Dr.Shaik Shakeer Basha[5], Dr.Keerthika T[6]

[1]Assistant Professor, Department of Computer Science and Engineering, BMS Institute of Technology and Management, Doddaballapur Main Road, Avalahalli, Yelahanka ,Bengaluru-560064.
[2]Assistant Professor, Department of Information Science and Engineering, BLDEA's V.P.Dr.P.G.Halakatti College of Engineering and Technology, Vijayapura-586103.
[3]Associate Professor, Department of Computer Science and Engineering, PSCMR College of Engineering and Technology, Vinchipeta, Vijayawada, Andhra Pradesh-520001.
[4]Assistant Professor, Department of Computer Science and Engineering, Vignan's Foundation for Science, Technology & Research(Deemed to be University), Vadlamudi, Guntur-522213,Andhra Pradesh.
[5]Assistant Professor, Department of Computer Science & Engineering, Avanthi Institute of Engineering and Technology, Gunthapally, Abdullahpurmet Mandal-501512, Hyderabad, Telangana.
[6]Assistant Professor, Department of Information Technology, Sri Krishna College of Engineering and Technology, Kuniamuthur, Coimbatore-641008.

Abstract -A blockchain is simply a shared database of information or public ledger of all completed and shared transactions or digital activities between cooperating occurrences. Each transaction in the public ledger is confirmed by a majority of the participants within the device. Data cannot be removed once it has been input. The blockchain is a secure and verifiable record of every single transaction ever made. The most popular example of blockchain generation is Bitcoin, a decentralize dpeer-to-peer digital currency. Although the virtual foreign currency bitcoin is debatable, the blockchain technology that underpins it has performed admirably. The main hypothesis is that the blockchain creates a system for reaching a distributed consensus in the virtual online world. By developing an irrefutable file in a public ledger, participating entities may be certain that avirtual event occurred. It paves the way for the development of a democratic, open, and scalable digital economy from a centralised one. This disruptive period offers incredible prospects, and the change in this field has only just begun. The blockchain age is described in this white paper, as well as some intriguing specific applications in the monetary and non-financial sectors. We then research the difficulties ahead of time as well as the commercial opportunities in this critical age.

Keywords:Blockchain, Chain cods, Risk, Issues, Mitigation

1. INTRODUCTION

A blockchain is essentially a shared database of data or public ledger of all completed transactions or digital events that may be shared among participants. Every transaction in the public ledger is verified by a majority of the device's members. Records can't be deleted once they've been submitted. The blockchain is a secure and verifiable record of all transactions that have ever taken place. To give a simple instance, stealing a cookie from a cookie jar kept in an isolated spot is far easier than stealing a cookie from a cookie jar kept in a market location and being discovered by hundreds of people.Bitcoin is the most well-known example of a cryptocurrency that is inextricably linked to blockchain development. It's also the most divisive because it allows for a multibillion-dollar global marketplace of anonymous transactions with no official oversight. As a result, it must deal with some regulatory issues relating to national governments and monetary institutions [1].

The Blockchain generation, on the other hand, is unquestionable and has performed admirably throughout time, and it is now being successfully used to both economic and non-economic world projects. MarcAndreessen, the doyen of Silicon Valley venture investors, named the blockchain-based consensusmodel as the most important investment opportunity in 2018.BNP Paribas' Johann Palychata said in Quintessence that bitcoin'sblockchain, the software programme that allows the virtualcurrency to function, should be viewed as an invention similar to the steam or combustion engine, with the potential to transform the world of finance and beyond [2]. The current digital financial system is founded on the trustworthiness of a positive authority.All of our onlinetransactions rely on trusting someone to tell us the truth—it could be an e-mail provider informing us that our e-mail has been introduced [3], a certification authority informing us that a certain digitalcertificate is valid, or a social network such as Facebook informing us that our postsabout our existence activities have been hacked. The truth is that we live precariously in the virtual world since we rely on a third party for our safety and privations.The reality is that these resources for the third celebration could be hacked, controlled, or hijacked [4].

This is where the blockchain generation may be found. It has the potential to transform the digital international by establishing a distributed consensus in which every online transaction, both past and present, involving digital property can be validated at any moment in the future. It accomplishes this by circumventing the privations of the virtual assets and parties involved. Blockchain technology is defined by its allocated consensus and anonymity [5].

2. LITERATURE REVIEW

Smart Property is a related concept that involves using blockchain and Smart Contracts to control the ownership of goods or assets. The belongings can be physical, such as a car, a house, or a cellphone. It can also be non-bodily inclusive of a business enterprise's stock. It is important to note that Bitcoin is not a foreign currency; rather, Bitcoin is all about managing the ownership of money.The blockchain era is bringing programmes to a wide number of industries, both financial and non-financial. Blockchain technology is no longer seen as a threat to existing business models by financial organisations and banks. The world's major banks are researching novel blockchain applications to see if there are any opportunities in this sector. Rain Lohmus of Estonia's LHV bank stated in a recent interview that they found Blockchain to be the most tested and comfortable for a number of banking and finance-related applications [7].

The possibilities for non-financial applications are likewise limitless.In the music industry, we might imagine storing evidence of all crime records, health information, and loyalty bills in the blockchain, as well as notaries, private securities, and marriage licences. The anonymity or privacy goal can be achieved by storing the fingerprint of the virtual asset instead of the virtual asset itself [8].

In the year 2008, Satoshi Nakamoto published a paper titled "Bitcoin: A Peer-to-Peer Electronic Cash System" under the pseudonym Satoshi Nakamoto. This paper defined a peer-to-peer model of digital coinage that might allow online invoices to be sent directly from one party to another without going through a financial institution.Bitcoin was the first to recognise this principle. Now, the term "cryptocurrency" is used to describe all networks and mediums of exchange that utilise cryptography to secure transactions—as opposed to those systems where transactions are routed through a centralised trusted institution. Because the first paper's author wished to remain anonymous, no one knows who SatoshiNakamoto is today. A few months later, an open source programme based on the new protocol was released, beginning with the Genesis block of fifty dollars. Anyone can instal and use this open source software to join the bitcoin peer-to-peer network. When you think about it, it's grown unnoticed.

Internet trading is solely dependent on financial institutions acting as trusted third parties to process and mediate each electronic transaction. The function of the 0.33 celebration is to validate, protect, and maintain transactions. A certain percentage of fraud is unavoidable in online transactions, necessitating financial transaction mediation. As a result, transaction costs are exorbitant. Instead of using the accept as true with inside the third birthday celebration for willing parties to execute a web transaction over the Internet, Bitcoin employs cryptographic evidence.A virtual signature is used to encrypt each transaction. Each transaction is sent to the receiver's "public key," which is digitally signed with the sender's "private key." To spend money, the owner of a cryptocurrency must show that he or she has the "private key." The entity receiving the digital foreign money validates the digital signature on the transaction using the sender's "public key" (therefore possessing a corresponding "non-public key").

3. BLOCKCHAIN WORKING MODEL:

Each transaction is broadcast to every node in the Bitcoin network and then verified before being recorded in a public ledger. Before a transaction can be recorded in the public ledger, it must first be confirmed to be valid. Before recording any transaction, the verifying node must ensure two things:

1. The spender owns the cryptocurrency, as evidenced by the transaction's digital signature verification.
2. Spender has enough cryptocurrency in his/her account: inside the ledger, examine each transactiontowards the spender's account ("public key") to ensure that he/she has enough cryptocurrency in his/her account.

   However, maintaining the order of transactions broadcast to each separate node inside the Bitcoin peer-to-peer network is a concern. Because the transactions are not public in the sequence in which they are generated, a computer may be required to ensure that double-spending of cryptocurrency does not occur.

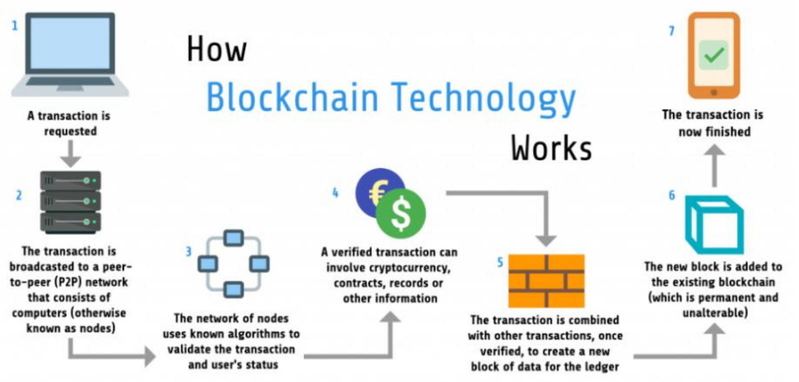
How
Blockchain Technology
Works
1
A transaction is requested
2
The transaction is broadcasted to a peer-to-peer (P2P) network that consists of computers (otherwise known as nodes)
3
The network of nodes uses known algorithms to validate the transaction and user's status
4
A verified transaction can involve cryptocurrency, contracts, records or other information
5
The transaction is combined with other transactions, once verified, to create a new block of data for the ledger
6
The new block is added to the existing blockchain (which is permanent and unalterable)
7
The transaction is now finished

Figure 1: Blockchain Technology – Process and Model

Because transactions are passed from node to node over the Bitcoin network, there is no guarantee that the orders gained at a node are the same as the order in which the transactions were generated. It's a data structure in which each block is linked to the next in a time-stamped chronological manner. It's an append-only transactional database that's no longer a replacement for traditional databases. Every node keeps a copy of all previous transactions, which are safeguarded cryptographically. All records are verifiable and auditable after they are saved in the ledger, but they are no longer editable. Because there is no single point of failure, it is extremely fault tolerant.

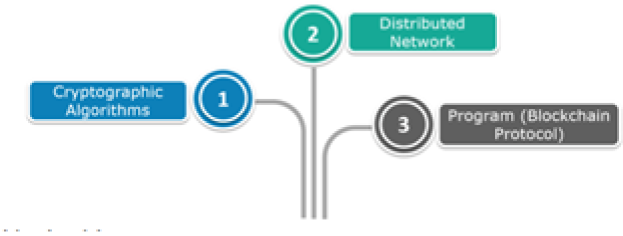

Figure 2: Input of Blockchain Model

Modern cryptographic mechanisms are used to secure blockchains. On the Blockchain, everything is encrypted. Let's return to our previously mentioned example, when Kevin transfers five BTC to James, to give you a better idea of how it's far used on Blockchain. This transaction will be broadcast to the community as an encrypted message. Every transaction receives a unique message. You might now wonder what distinguishes the message. Because the transaction is signed using the sender's unique key, known as a non-public key, the virtual signature is created. The mechanism appears to be as follows:

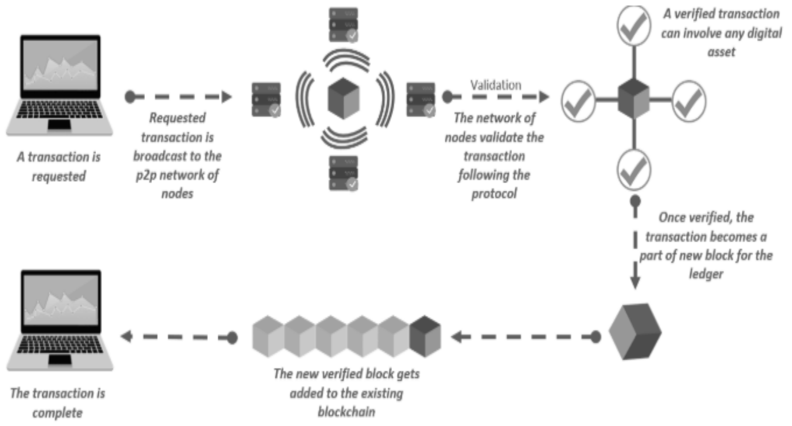
A transaction is requested
Requested transaction is broadcast to the p2p network of nodes
Validation
The network of nodes validate the transaction following the protocol
A verified transaction can involve any digital asset
Once verified, the transaction becomes a part of new block for the ledger
The new verified block gets added to the existing blockchain
The transaction is complete

Figure 3: Cryptography Mechanism

4. FINANCIAL MODEL

- Medici is being developed as a securities trading that makes advantage of Bitcoin 2.0's Counterpartyimplementations. The goal is to build a marketplace with a smaller inventory area. Counterparty is a system for converting traditional financial instruments into self-executing smart contracts. These ingenious contracts eliminate the need for a physical record by facilitating, verifying, or enforcing the agreement. This eliminates the need for a middleman, such as a dealer, exchange, or financial institution.
- Blockstream is an open source project that keeps track of sidechains—interoperableblockchains—to avoid fragmentation, security, and other concerns that come with opportunity crypto-currencies. Securities, such as stocks, bonds, and derivatives, can be registered, as well as bank balances and mortgages.
- Coinsetter is a bitcoin exchange situated in New York. It is developing Project Highline, a way of using the blockchain to settle and clear monetary transactions in T+ 10 minutes rather than the usual T+ 3 or T+ 2 days.
- Augur is a decentralised prediction marketplace that allows users to purchase and sell shares in advance of an event with the probability of a specific outcome. This can also be used to produce monetary and economic forecasts based on "crowd-sourced knowledge."
- Bitshares are digital tokens that exist within the blockchain and correspond to specific assets such as cash or commodities. Token holders may also be able to earn income on commodities such as gold and oil, as well as greenbacks, euros, and foreign exchange contracts.
- Stampery is a company that uses blockchain to stamp e-mails and other files. It simplifies email certification by simply emailing them to a custom-created electronic mail address for each customer. Stampery's era is being used by law firms as a cost-effective way to certify documents.
- Viacoin is one of the companies that uses the clearinghouse protocol to provide notary services.
- Block Notary is an iOS app that uses the TestNet3 or Bitcoin networks to create proof of existence for any material (pictures, files, or other media).
- Crypto Public Notary is a service that uses the BitcoinBlockchain to notarize documents by using a small amount of bitcoins to register the record's checksum on the public blockchain.

- Every other carrier that uses blockchain to SHA256 digest of the record in the bitcoinblockchain is known as Proof of Existence.
- Ascribe is another another company that uses blockchain to perform authorship certification. It also provides ownership transfer with attribution to the original creator.

5. ISSUES AND RISK

- BlockChain is a promising next-generation technology. As previously stated, BlockChain-based technology can be used to solve a wide range of applications or issues. This includes everything from financial (remittances to investment banking) to non-financial (notary services). The majority of these are significant enhancements. There are significant risks of acceptance, just as there are with radical inventions.
- Behavioral trade: Change occurs on a regular basis, but there is resistance to change. Customers must become accustomed to the fact that their electronic transactions are secure, secure, and complete in the world of a non-tangible, trusted third party, which BlockChain provides.
- Modern middlemen, such as Visa or Mastercard (in the case of credit cards), may even take on different duties and responsibilities. We believe they will invest in and pass their systems to be entirely BlockChain-based. They will continue to deliver customer relationship-oriented services.
- Scaling: Scaling of cutting-edge fledgling BlockChain solutions allows for assignment. Consider the first time you carried out a BlockChain transaction. Before conducting your first transaction, you need download the entire collection of existing BlockChains and validate them. As the number of blocks grows exponentially, this could take hours or even days.
- Bootstrapping: Migrating existing contracts or business files/frameworks to the new BlockChain-based technique necessitates a large number of operations. For example, in the case of real estate ownerships/liens, the current documents held by County or Escrow organisations should be converted to the BlockChain equivalent. This could also include information on the date and pricing.

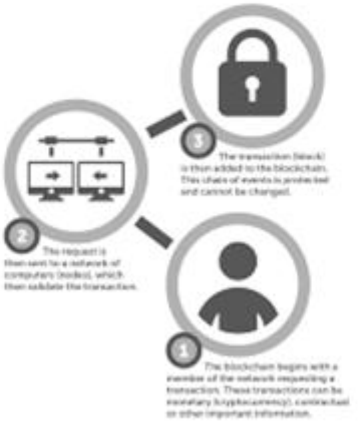
3
The transaction (block) is then added to the blockchain. This chain of events is protected and cannot be changed.
2
The request is then sent to a network of computers (nodes), which then validate the transaction.
1
The blockchain begins with a member of the network requesting a transaction. These transactions can be monetary (cryptocurrency), contractual or other important information.

Figure 4: Risk Management in Blocks

- Government Regulations: In the new world of BlockChain-based completely transactions, government agencies such as the FTC, SEC, and others can stifle adoption by enacting new regulations to monitor and change the industry for compliance. This can help adoption in the United States because these companies provide consumer trust. Adoption will confront significant challenges in extra-managed economies like as China.
- Fraudulent Activities: Due to the pseudonymous nature of BlockChain transactions, along with the ease with which they can move goods, the heinous men may also use it for fraudulent activities such as currency trafficking. That said, law enforcement groups can filter and prosecute them with adequate legislation and eraguide.
- Quantum Computing: The foundation of BlockChain generation is based on the fact that due to a lack of required compute energy, it is theoretically impossible for a single birthday party to host the system. However, with the advent of Quantum Computers (in the future), cryptographic keys may become clean enough to crack using the brute-force method in a reasonable amount of time. This will bring the entire device to a halt. The counter-argument is that keys should get more powerful so that they are more difficult to crack.

6. SOLUTIONS AND MITIGATIONS

A. Anti-Counterfeit Solution:

BlockVerify offers anti-counterfeiting solutions based on the blockchain that bring transparency to supply chains. It's used in the pharmaceutical, luxury goods, jewels, and electronics industries. The pharmaceutical business, for example, can employ BlockVerify anti-counterfeit systems to prevent fake drugs from entering the market.This covers a major issue that has ramifications for both the economy and those who require medication. Similarly, luxurious precise producers can leverage this technology to create a gadget that verifies the authenticity of luxury goods, creating a win-win situation for both customers and luxury goods manufacturers. This technique can be used by the diamond industry to build trust in diamond certificates and avoid fraud. This technology can be used in the electronics industry to ensure that customers receive genuine items.

B. Chain Link:

Any industry can utilise the BlockVerify era to define a process for ensuring the authenticity of its products. The following is how BlockVerify operates:

- A Block Verify tag is attached to each product.
- Even corporations are prevented from counterfeiting their personal things because each product is validated and logged in the BlockChain.
- To verify each product, the supply chain uses BlockChain creation.
- Mobile devices can be used in retail venues to verify the authenticity of products purchased.
- Similarly, a customer looking for a goods might check to see whether it is genuine and then ignite it.

Each product has a record that is permanently stored in the blockchain, allowing everyone in the supply chain to verify the product's authenticity. ChainLink is another anti-counterfeiting tool that uses coloured banknotes to prevent counterfeit luxury products, such as handbags and watches, from entering the market. By adding a layer of accept as true with to secondary markets like eBay and Craigslist, the carrier makes them safer.

C. Distributed Storage

As it stands now, cloud storage relies on data carriers to carry out each transaction. It demonstrates the traditional cloud-based completely storage architecture for transferring and saving data via dependable cloud carrier carriers like Googleforce, Dropbox, and One pressure. They adhere to industry standards for redundancy by storing several copies of the records (usually 3 copies). However, because there is no well-known method of performing end-to-end encryption, traditional cloud-based architecture is vulnerable to a wide range of security threats, including malware, man-in-the-middle attacks, and alertness hacks, which could expose sensitive and personal customer or company information.

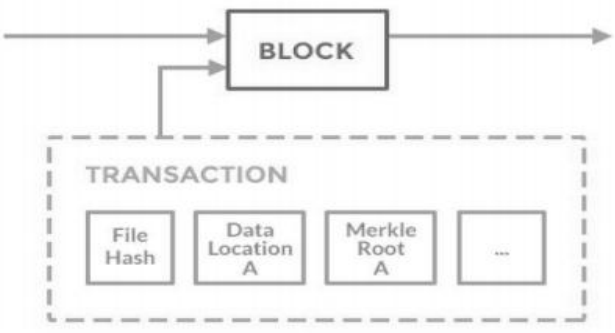

Figure 6: Metadata model of each blocks

The difficulties of the traditional garage community can be addressed by implementing a peer-to-peer cloud storage community with continuous encryption, allowing users to safely transmit and share information without relying on a third party for security and reliability. It eliminates reliability because there is no reliance on a third party, and hence traditional information breakdowns and outages are eliminated. Furthermore, it significantly increases the statistics' security and privacy.

7. CONCLUSION

Finally, Bitcoin's generation spine is Blockchain. The dispensedledger feature, together with BlockChain's security, makes it a very appealingera for resolving existing financial and non-financial business issues. In terms of the generation, cryptocurrency-based technology is either on the upward slope of inflated expectations or in the trough of disillusionment. There is a lot of interest in BlockChain-based commercial applications, and as a result, there are a lot of startups working on them. As previously said, the adoption confronts a strong headwind.Large financial institutions including as Visa, Mastercard, Banks, NASDAQ, and others are investing in researching the use of modern business models on BlockChain. In fact, a number of them are looking for new business models in the world of BlockChain. Some people would desire to be ahead of the curve when it comes to BlockChain's altered regulatory settings. To sum up, we expect BlockChain adoption to be slow due to the risks involved. The majority of startups will fail, with only a few exceptions. In a decade or two, we should see widespread adoption.

8. REFERENCES:

[1] Morgen Peck, Freelance Technology Writer, Contributing Editor of IEEE Spectrum Magazine Special Edition “Blockchain World”, 2017

[2] William R. Tonti, Director, IEEE Future Directions • AngelosStavrou, Professor, Computer Science Department, George Mason University • Jason W. Rupe, Director, Operational Modelling, Polar Star Consulting • ChunmingRong, Head, Center of IP-based Services Innovation (CIPSI) • Tim Kostyk, IEEE Future Directions REINFORCING THE LINKS OF THE BLOCKCHAIN, IEEE future directions blockchain initiative white paper blockchainincubator.IEEE.ORG, 2017

[3] Bitcoin: A Peer-to_peer Electronic Cash System

[4] Smart Contracts: Nick Szabo

[5] Formalizing and Securing Relationships on Public Networks: Nick Szabo

[6] Introduction To Smart Contracts

[7] The Ultimate List of Bitcoin and Blockchain White Papers

[8] Bitcoin Tutorial 7. A Risk-Based View of Why Banks are Experimenting with Bitcoin and the Block Blockchain:The Information Technology of The Future

[9] Bitcoin 2.0 Applications

[10] Beyond Bitcoin:How the Blockchain Can Power a New Generation of Enterprise Software

[11] Forget Bitcoin-What is the Blockchain and Why Should You Care?

[12] https://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf

[13] https://blockchain.ieee.org/images/files/pdf/ieee-future-directions-blockchain-white-paper.pdf

[14] https://blockgeeks.com/guides/what-is-blockchain-technology/

[15] www.ibm.com/IBM/Solutions

[16] builtin.com › blockchain

[17] https://www.investopedia.com/terms/b/blockchain.asp